



# AREA MARITIME SECURITY PLAN for NORTHEAST and EASTERN CENTRAL FLORIDA



Developed by the  
JMTX Port Security Committee  
and  
Port Canaveral Security Committee

SENSITIVE SECURITY  
INFORMATION REMOVED  
26 May 2004



**[This Page Intentionally Left Blank]**

# TABLE OF CONTENTS

1000	<u>AREA MARITIME SECURITY</u>	1000-9
1100	<u>Purpose</u>	1000-9
1200	<u>Letter of Promulgation</u>	1000-11
1210	<u>Record of Changes</u>	1000-12
1300	<u>Authority</u>	1000-15
1310	<u>Federal Maritime Security Coordinator</u>	1000-15
1400	<u>Scope</u>	1000-15
1500	<u>Suppositions</u>	1000-16
1600	<u>Situation</u>	1000-17
1610	<u>Physical Characteristics</u>	1000-17
1611	<u>Northeast and Eastern Central Florida Area</u>	1000-18
1612	<u>St. Marys River and Fernandina</u>	1000-18
1613	<u>St. Johns River and Jacksonville</u>	1000-22
1614	<u>Intracoastal Waterway and Coastline</u>	1000-34
1615	<u>Port Canaveral</u>	1000-39
1620	<u>Economic Characteristics</u>	1000-43
1621	<u>Fernandina, Florida, and Kings Bay, Georgia</u>	1000-43
1622	<u>Jacksonville, Florida</u>	1000-44
1623	<u>Port Canaveral, Florida</u>	1000-45
1630	<u>Port Charts and Maps</u>	1000-46
1631	<u>Northeast and Eastern Central Florida Area</u>	1000-46
1632	<u>St. Marys River and Fernandina</u>	1000-46
1633	<u>St. Johns River and Jacksonville</u>	1000-46
1634	<u>Intracoastal Waterway and Coastline</u>	1000-46
1635	<u>Port Canaveral</u>	1000-46
1636	<u>Population Density Maps</u>	1000-46
1636.1	<u>Nassau County Population Density</u>	1000-48
1636.2	<u>Duval County Population Density</u>	1000-49
1636.3	<u>St. Johns Population Density</u>	1000-50
1636.4	<u>Volusia County Population Density</u>	1000-51
1636.5	<u>Brevard County Population Density</u>	1000-52
1640	<u>Information Characteristics</u>	1000-53
1700	<u>Links to Other Federal, State, and Local Plans</u>	1000-53
1710	<u>Federal Security and Response Plans</u>	1000-53
1711	<u>National Response Plan</u>	1000-53
1712	<u>U.S. Govt Interagency Domestic Terrorism CONOP</u>	1000-54
1713	<u>Federal Response Plan</u>	1000-54
1714	<u>Federal Radiological Response Plan</u>	1000-55
1715	<u>National Oil and Hazard Substances Pollution Cont Plan</u>	1000-56

	1716 Department of Defense Plans _____	1000-56
	1720 Florida State and Local Security Response Plans _____	1000-57
	1730 Georgia State and Local Security Response Plans _____	1000-57
	1740 Vessel and Facility Security Plans _____	1000-58
2000	AREA MARITIME SECURITY COMMITTEE _____	2000-1
2100	Introduction _____	2000-1
2200	Purpose and Objectives _____	2000-2
2300	Charter _____	2000-2
	2310 Organization _____	2000-2
	2311 JMTX Jacksonville/Fernandina Port Security Committee ____	2000-3
	2312 Port Canaveral Security Committee _____	2000-3
	2313 Standing Subcommittees _____	2000-4
	2314 Ad-Hoc Subcommittees _____	2000-4
	2320 Rules Governing Port Security Committees _____	2000-4
	2321 Purpose and Scope of the Committees _____	2000-4
	2322 Membership in the Committees _____	2000-5
	2323 Meetings of the Committees _____	2000-5
	2324 Geographic Area of Responsibility of the Committees ____	2000-5
	2330 Rules Governing Working Subcommittees _____	2000-6
	2331 Purpose and Scope of the Working Subcommittees _____	2000-6
	2332 Membership in the Subcommittees _____	2000-7
	2333 Officers of the Subcommittees _____	2000-7
	2334 Meetings of the Subcommittees _____	2000-7
	2335 Working Subcommittee Procedural Rules _____	2000-7
	2340 Rules Governing the Executive Subcommittees _____	2000-8
	2341 Purpose and Scope of the Executive Subcommittee _____	2000-8
	2342 Membership in the Executive Subcommittee _____	2000-9
	2343 Nomination and Appointment Process _____	2000-10
	2344 Acceptance and Pledge _____	2000-10
	2345 Officers of the Executive Subcommittee _____	2000-11
	2346 Schedule of Meetings _____	2000-11
	2347 Executive Subcommittee Procedural Rules _____	2000-11
	2350 Handling and Protecting Information _____	2000-13
	2351 Rules for SSI Sessions and SSI Information _____	2000-14
	2352 Rules for Classified Sessions and Classified Information ____	2000-15
	2353 Rules for Commercially Sensitive Information _____	2000-15
	2354 Rules for Proprietary Information _____	2000-15
	2360 Amending the Charter _____	2000-15
2400	Relationship to Other Committees _____	2000-15

3000	AWARENESS	3000-1
3100	Introduction	3000-1
3200	Federal, State & Local Security & Law Enforcement Agency Jurisdiction	3000-1
3300	Area Maritime Security (AMS) Assessment	3000-17
3310	Maritime Security Assessment Report	3000-17
3320	Critical Marine Transportation Infrastructure and Operations	3000-17
3330	Area Maritime Security Threat Assessment	3000-21
3340	Area Maritime Security Assessment	3000-22
3350	(SSI) Security Measures for MARSEC 1, 2 and 3	3000-25
3400	Communications	3000-25
3410	Communication of Security Information	3000-26
3410.1	Communication with the Public	3000-27
3410.2	Communications with Waterway Users (Boaters)	3000-30
3410.3	Communications with Commercial Vessels	3000-33
3410.4	Communications with Facilities	3000-36
3410.5	Communications with Companies	3000-38
3410.6	Role of the Port Security Committees	3000-39
3420	Security Reporting	3000-39
3420.1	Procedures for Reporting Suspicious Activity	3000-40
3420.2	Procedures for Reporting Security Breaches	3000-40
3420.3	Procedure for Reporting Transportation Security Incidents	3000-40
3430	Communicating MARSEC Directives	3000-41
3430.1	Procedures for Communicating Security Directives	3000-41
3430.2	Procedures for Responding to MARSEC Directives	3000-43
3430.3	Role of the Port Security Committees	3000-45
3440	Communicating MARSEC Levels	3000-46
3440.1	Procedures to Communicate Changes in MARSEC Levels	3000-46
3440.2	Reporting Attainment of MARSEC Levels	3000-47
3440.3	Role of the AMS Committee	3000-49
3500	Sensitive Security Information	3000-49
3510	Information Constituting Security Sensitive Information	3000-49
3520	Covered Persons	3000-52
3520.1	Designation as a Covered Person	3000-52
3530	Restrictions on the Disclosure of SSI	3000-53
3540	Persons with a Need to Know	3000-53
3550	Marking of SSI	3000-54
3560	SSI disclosed by TSA or the USCG	3000-54
3570	Consequences of Unauthorized SSI Disclosure	3000-55
3580	Destruction of SSI	3000-55
3590	Procedures for Communicating SSI Material	3000-55
3600	Maritime Security Training	3000-56

3700	Security Resources _____	3000-57
4000	PREVENTION _____	4000-1
4100	Introduction _____	4000-1
4200	Maritime Security (MARSEC) Level Planning _____	4000-2
	4210 Link to Homeland Security Advisory System _____	4000-2
	4220 Procedures when a vessel & facility at different MARSEC levels _	4000-3
	4230 Procedures for Requesting Equivalencies to MARSEC Directives	4000-4
4300	MARSEC Level 1 _____	4000-5
	4310 Roles, Resources, Authorities and Responsibilities _____	4000-5
	4320 Standard Security Procedures _____	4000-5
	4330 (SSI) Physical Security Measures _____	4000-5
	4340 (SSI) Operational Security (OPSEC) Measures _____	4000-16
	4350 (SSI) Security Measures for SPOE Operations _____	4000-17
4400	MARSEC Level 2 _____	4000-19
	4410 Roles, Resources, Authorities and Responsibilities _____	4000-19
	4420 Standard Security Procedures for MARSEC TWO _____	4000-19
	4430 (SSI) Physical Security Measures _____	4000-20
	4440 (SSI) Operational Security (OPSEC) Measures _____	4000-30
	4450 (SSI) Security Measures for SPOE Operations _____	4000-32
4500	MARSEC Level 3 _____	4000-34
	4510 Roles, Resources, Authorities and Responsibilities _____	4000-34
	4520 Standard Security Procedures for MARSEC THREE _____	4000-34
	4530 (SSI) Physical Security Measures _____	4000-35
	4540 (SSI) Operational Security (OPSEC) Measures _____	4000-38
	4550 (SSI) Security Measures for SPOE Operations _____	4000-40
4600	Public Access Facility _____	4000-41
	4610 Designation of Public Access Facilities _____	4000-41
	4611 Designated Public Access Facilities _____	4000-41
	4612 Review and Evaluation of PAF Exemption Request _____	4000-42
	4613 Establishment of Conditions _____	4000-42
	4614 Issuance of PAF Designation _____	4000-42
	4620 Vessel Responsibilities when Calling at a PAF _____	4000-43
	4621 General Responsibilities _____	4000-43
	4622 MARSEC ONE Responsibilities _____	4000-43
	4623 MARSEC TWO Responsibilities _____	4000-44
	4624 MARSEC THREE Responsibilities _____	4000-44
	4630 Compliance and Enforcement _____	4000-44
	4631 Submission of PAF Exemption Requests _____	4000-44
	4632 Action on Requests _____	4000-45
	4633 Annual Review _____	4000-45

	4634 Enforcement Action _____	4000-45
4700	Maritime Worker Credentials _____	4000-46
5000	PREPAREDNESS FOR RESPONSE _____	5000-1
5100	Introduction _____	5000-1
	5110 Procedures for responding to suspicious activity _____	5000-1
	5120 Procedures for responding to breaches in security _____	5000-3
5200	Transportation Security Incident (TSI) _____	5000-3
	5210 Procedures for Notification _____	5000-3
	5220 Incident Command Activation _____	5000-4
	5230 Threats that Do Not Rise to the Level of a TSI _____	5000-4
5300	Most Probable Transportation Security Incident _____	5000-4
	5310 Identify Command Structure with assigned roles (ICS flowchart) _____	5000-5
	5320 Procedure for responding to TSI _____	5000-5
	5330 Linkage with applicable Federal, State, Port, & Local plans _____	5000-6
5400	Maritime Security Exercise Requirements _____	5000-7
	5410 Purpose of Exercise Program _____	5000-7
	5420 Goals of the AMS Exercise Program _____	5000-8
	5430 Exercise cycle _____	5000-8
	5440 Scheduling and design _____	5000-9
	5450 Consideration of equivalent response _____	5000-10
	5460 Recordkeeping _____	5000-10
	5470 Linkages between Family of Plans within the Area _____	5000-10
6000	CONSEQUENCE MANAGEMENT AND RECOVERY _____	6000-1
6100	Introduction _____	6000-1
6200	Procedures to Maintain Infrastructure _____	6000-2
	6210 (SSI) Major Transportation Routes _____	6000-2
	6211 (SSI) Attack on a Bridge _____	6000-2
	6212 (SSI) Waterway Obstruction _____	6000-3
	6220 (SSI) Military Critical Shipping Channels _____	6000-4
	6230 (SSI) Military Critical Port Areas _____	6000-4
	6240 (SSI) Secondary Transportation Routes _____	6000-4
	6250 (SSI) Commercially Critical Shipping Channel _____	6000-4
	6260 (SSI) Attack on a Shoreside Facility _____	6000-4
	6270 (SSI) Vessel Explosion in a Waterway _____	6000-5
6300	Procedures for Recovery of MTS _____	6000-6
7000	COMPLIANCE MEASURES _____	7000-1
7100	Introduction _____	7000-1
7200	Reserved _____	7000-2

<u>8000</u>	PLAN DOCUMENTATION AND MANAGEMENT	8000-1
8100	Initial Plan Review and Comment	8000-1
8110	Procedures for continuous review and update of AMS Plan	8000-2
8110.1	Annual Informal Review	8000-2
8110.2	Formal Review	8000-3
8110.3	Perishable Information Management	8000-3
8110.4	Submission of Updates	8000-3
8120	Procedures for Cont Review and Update of the AMS Assessment	8000-3
<u>9000</u>	APPENDICES	9000-1
9100	Elements of Maritime Homeland Security	9100-1
9110	Elements of PWCS	9100-1
9111	Anti-Terrorism	9100-1
9112	Counter-Terrorism	9100-1
9113	Response to Terrorism	9100-1
9120	Terrorism	9100-2
9121	Terrorist Tactics	9100-2
9122	Terrorist Groups	9100-6
9123	Terrorist Organization	9100-6
9124	Terrorist Targets – Americans	9100-8
9125	Domestic Terrorism	9100-9
9200	Port Security Committee Executive Subcommittee Members	9200-1
9300	Charts and Maps of Port Areas	9300-1
9300.1	COTP Jacksonville Zone	9300-2
9300.2	Downtown Jacksonville	9300-3
9300.3	Lower St. Johns River	9300-4
9300.4	Port Canaveral	9300-5
9300.5	Port Fernandina	9300-6
9400	AMS Assessment	AMS-1
9500	Communications	9500-1
	TAB A: (SSI) ICS 205 Comm Plan	9500A-1
	TAB B: Vessel Contact Information	9500B-1
	TAB C: Facility Contact Information	9500C-1
	TAB D: Company Contact Information	9500D-1
	TAB E: Communications with Marinas	9500E-1
	TAB F: Communications with County Emergency Operations Centers	9500F-1
	TAB G: Communications with Waterway Users (Boaters)	9500G-1
	TAB H: MSIB to set MARSEC TWO	9500H-1
	TAB I: MSIB to set MARSEC ONE	9500I-1
	TAB J: MSIB to set MARSEC THREE (From MARSEC ONE)	9500J-1



	TAB K: MSIB to set MARSEC THREE (From MARSEC TWO)	9500K-1
	TAB L: MSIB to set MARSEC TWO (From MARSEC THREE)	9500L-1
	TAB M: BNTM to set MARSEC ONE	9500M-1
	TAB N: BNTM to set MARSEC TWO	9500N-1
	TAB O: BNTM to set MARSEC THREE	9500O-1
	TAB P: (SSI) MJTF Notification Procedures	9500P-1
	TAB Q: MARSEC E-Mail Notification Template	9500Q-1
9600	Security Incident Response Procedures	9600-1
	TAB A: (SSI) SA-1 Bomb Threat	9600A-SA1-1
	(SSI) SA-2 Access Attempt	9600A-SA2-1
	(SSI) SA-3 Photos/Surveillance	9600A-SA3-1
	(U) SA-1 Bomb Threat	9600A-SA1-1
	(U) SA-2 Access Attempt	9600A-SA2-1
	(U) SA-3 Photos/Surveillance	9600A-SA3-1
	TAB B: (SSI) SB-1 Trespass and Stowaway	9600B-SB1-1
	(SSI) SB-2 Small Illegal Protest	9600B-SB2-1
	(SSI) SB-3 Security System Tampering	9600B-SB3-1
	(SSI) SB-4 Security Measure not Implemented	9600B-SB4-1
	(U) SB-1 Trespass and Stowaway	9600B-SB1-1
	(U) SB-2 Small Illegal Protest	9600B-SB2-1
	(U) SB-3 Security System Tampering	9600B-SB3-1
	(U) SB-4 Security Measure not Implemented	9600B-SB4-1
	TAB C: (SSI) TSI-1 Rogue Vessel	9600C-TSI 1-1
	(SSI) TSI-2 CBR Terrorism	9600C-TSI 2-1
	(SSI) TSI 3 Explosive Device/IED Detected or Suspected	9600C-TSI 3-1
	(SSI) TSI 4 Armed Trespass	9600C-TSI 4-1
	(SSI) TSI 5 Suspect Cargo	9600C-TSI 5-1
	(SSI) TSI 6 Suspect Employee	9600C-TSI 6-1
	(SSI) TSI 7 Explosion in Port	9600C-TSI 7-1
	(SSI) TSI 8 Large Illegal Protest	9600C-TSI 8-1
	(SSI) TSI 9 Port Mass Evacuation	9600C-TSI 9-1
	(U) TSI-1 Rogue Vessel	9600C-TSI 1-1
	(U) TSI-2 CBR Terrorism	9600C-TSI 2-1
	(U) TSI 3 Explosive Device/IED Detected or Suspected	9600C-TSI 3-1
	(U) TSI 4 Armed Trespass	9600C-TSI 4-1
	(U) TSI 5 Suspect Cargo	9600C-TSI 5-1
	(U) TSI 6 Suspect Employee	9600C-TSI 6-1
	(U) TSI 7 Explosion in Port	9600C-TSI 7-1
	(U) TSI 8 Large Illegal Protest	9600C-TSI 8-1
	(U) TSI 9 Port Mass Evacuation	9600C-TSI 9-1
	TAB D: GSTRAP [RESERVED]	9600D-1

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-7
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

9700	MJTF Incident Action Templates _____	9700-1
	TAB A: (SSI) MARSEC ONE [RESERVED] _____	9700A-1
	TAB B: (SSI) MARSEC TWO _____	9700B-1
	TAB C: (SSI) MARSEC THREE [RESERVED] _____	9700C-1
	TAB D: (SSI) Military Outload _____	9700D-1
	TAB E: (SSI) Major Marine Event [RESERVED] _____	9700E-1
9800	Glossary of Terms _____	9800-1
9900	Interagency Agreements _____	9900-1
	9910 Signed Port Security Committee Charter _____	9910-1
	9920 Maritime Joint Task Force _____	9920-1
	9930 Port Facilities Form Details _____	9930-1
	9940 Public Access Facilities _____	9940-1
10000	Dangerous Cargoes for Security Planning _____	10000-1
	10010 Introduction _____	10000-1
	10011 Implications of Dangerous Cargoes in Security Planning__	10000-1
	10012 Scenario Based Planning _____	10000-1
	10012.1 Hazard Analysis and Inventory _____	10000-1
	10020 Database of Dangerous Cargoes _____	10000-2

## 1000 Area Maritime Security

This section outlines the overall area maritime security framework. This section of this plan has been organized into the following subsections (click on the link to view the section) :

1100	<a href="#">Purpose</a>
1200	<a href="#">FMSC Promulgation Letter</a>
1210	<a href="#">Record of Changes</a>
1300	<a href="#">Authority</a>
1400	<a href="#">Scope</a>
1500	<a href="#">Suppositions</a>
1600	<a href="#">Situation</a>
1700	<a href="#">Federal Maritime Security Coordinator</a>
1800	<a href="#">Links to Other Federal, State, and Local Security and Response Plans</a>

## 1100 Purpose

The Coast Guard is the Lead Federal Agency (LFA) for Maritime Homeland Security. The Captain of the Port (COPT), as the Federal Maritime Security Coordinator (FMSC) is responsible for developing an Area Maritime Security (AMS) Plan, with advice from the Port Security Committees. The Port Security Committees for Northeast and Eastern Central Florida have created this AMS plan. It is designed to deter, to the maximum extent possible, a transportation security incident (TSI). This AMS Plan defines the government's (local, state, and federal) obligations, and the contributions and responsibilities of other port stakeholders, to the Maritime Homeland Security (MHS) mission.

A primary purpose of this AMS plan is to provide a framework for communication and coordination amongst port stakeholders and law enforcement officials, and to identify and reduce vulnerabilities to security threats in and near the Maritime Transportation System (MTS). This AMS Plan has been designed to capture the information necessary to coordinate and communicate security procedures at each Maritime Security (MARSEC) Level. It complements Facility and Vessel Security Plans within the COTP zone and is fully integrated with the National Maritime Security Plan.

Pursuant to this AMS plan, MTS stakeholders will take certain actions contingent upon changes in MARSEC Levels and develop unified preparedness strategies to deter and respond to security incidents. A TSI is defined in the Maritime Transportation Security Act (MTSA) as "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Examples of a TSI may include:

- (1) An incident affecting a particular mode of transportation or inter-modal structure that significantly disrupts normal operations or may result in closure for a significant time period of a key terminal, waterway, or part of the MTS or
- (2) An actual incident, such as an explosion, MTS blockage, release of a Weapon of Mass Destruction (WMD), hijacking, etc.

Not every threat or incident that violates a security plan, process or perimeter, will necessarily result in a TSI. In creating this AMS plan, efforts focused on identifying and implementing measures designed to prevent the occurrence of TSI's. Threats and violations need to be evaluated on a case-by-case basis and responded to accordingly. It is the FMSC's responsibility to determine if and when an incident occurring in his or her zone is severe enough to warrant designation as a TSI.

33 CFR 103.200 designates Captain of the Ports (COTP) as Federal Maritime Security Coordinators

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-9
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

(FMSC) for their respective COTP zones. For practical purposes, this AMS Plan uses the terms FMSC and COTP interchangeably, it does not change the authorities granted to the COTP or FMSC under relevant statutes or regulations.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-10
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1200 Letter of Promulgation

### AREA MARITIME SECURITY PLAN for NORTHEAST AND EASTERN CENTRAL FLORIDA LETTER OF PROMULGATION

1. **Purpose.** The Area Maritime Security Plan for Northeast and Eastern Central Florida provides local information, specific security measures, a security incident response organization, and detailed plans for responding to transportation security incidents. It was developed to coordinate with local, regional, and national-level multi-organization terrorism prevention and response (security) plans.
2. **Publications Affected.** This plan is effective immediately and supercedes all previous maritime security agreements and plans.
3. **Discussion.** This plan includes information on general authority, doctrine/policy for security and response, assignment of responsibilities, multi-agency response organization, and specific security incident response actions.
4. **Action.** The Commander, Coast Guard Atlantic Area approved this plan on **DATE** . The Northeast Florida Area Maritime Security Plan is the unified policy to be followed by all entities in the Northeast Florida area while conducting preventive security actions and during responses to actual security incidents. All port entities shall assure that personnel performing these duties are trained and qualified to comply with its provisions.

**D. L. Lersch**

D. L. LERSCH  
Captain, U.S. Coast Guard  
Federal Maritime Security Coordinator

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-11
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1210 Record of Changes

This plan is under the control of the Federal Maritime Security Coordinator for Northeast and Eastern Central Florida. Within the context of updates and changes to this plan, no person other than the Federal Maritime Security Coordinator is authorized to make changes to the plan. The Federal Maritime Security Coordinator will continuously update this plan in accordance with section 8000 (series) of this plan.

When an update is reviewed and approved as outlined in section 8000, the Federal Maritime Security Coordinator will issue a Change Distribution letter. This Change Distribution letter will detail which sections have been replaced and provide new insert pages marked with a new version/date in the lower left hand corner. Where unclassified sections of the plan are changed, the Distribution Letter will be unclassified and posted for public consumption. Where Sensitive Security Information sections of the plan are changed, the Distribution Letter will reference an SSI-level addendum specifying and conveying these changes. The SSI-level addendum will not be generally available, and will be transmitted ONLY to those entities deemed both covered and with a need-to-know. The SSI-level addendum will be marked, handled, protected, and transmitted in accordance with section 3500 of this plan. When a change contains ONLY SSI information, the Change Distribution letter will remain at the unclassified level, contain no summary, and refer solely to the SSI-level addendum. In this fashion, any person who believes they are a covered person with a need-to-know will be aware of the change and may contact the FMSC's staff to receive the SSI-level addendum.

All holders of this plan, whether at the fully unclassified level or the Sensitive Security Information level, are directed to monitor for Change Distribution letters and when receiving such a letter, are required to make the changes in the letter and/or SSI-level addendum. No other changes to the plan are authorized. When a change has been made in accordance with the Change Distribution letter, the plan holder must log the entry of the change into the plan itself; a change log form follows this section. In the case of paper copies of the plan, the old sections should be removed and destroyed (SSI destruction rules are in section 3500 of this plan), and the newly distributed changes should be inserted. For electronic distributions, the old files must be overwritten with the newly distributed changes. Old electronic copies should be deleted.

Where a person concludes that a change to this plan is necessary, advisable, or desired, that entity should submit a change request to the Federal Maritime Security Coordinator. Such change requests will be consolidated, reviewed and evaluated by the Port Security Committees, and (as approved) acted upon by the Federal Maritime Security Coordinator. Following the Record of Changes, a Change Submission form can be found.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-12
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

# CHANGE RECORD FORM

[illegible]

# CHANGE SUGGESTION FORM

**Date Submitted to the FMSC:**

**From (name):**

**Contact e-mail and phone (optional):**

**To: JMTX Port Security Committee and Port Canaveral Security Committee**

**Via: Federal Maritime Security Coordinator**

[illegible]



## 1300 Authority

Section 102 of the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295, codified at 46 USC Sections 70101 – 70117, mandates the development of a National Maritime Transportation Security Plan, Area Maritime Security Plans, and Facility and Vessel Security Plans. The Coast Guard is designated as the Lead Federal Agency (LFA) responsible for implementation of the MTSA. The COTP's, acting as Federal Maritime Security Coordinators (FMSC), are responsible for developing AMS Plans with advice from AMS Committees. In the development of this AMS Plan, the FMSC has solicited advice from the two regional Port Security Committees, as required under Federal regulations. This AMS Plan is consistent with the National Maritime Transportation Security Plan and the National Transportation Security Plan.

See:

- 46 USC 70103(b) & ISPS
- 33 CFR 103
- NVIC 09-02 Change 1

## 1310 Federal Maritime Security Coordinator

The Captain of the Port, Jacksonville FL, is designated as the FMSC, charged with the responsibility of establishing an AMS Committee and developing an AMS Plan. These security responsibilities are in addition to key responsibilities for traditional Coast Guard missions and are fundamental to the success of the maritime homeland security program. To accomplish the goals outlined in the Coast Guard's Maritime Strategy for Homeland Security, the FMSC must rely on fellow Federal, State, and local representatives and other maritime agency partners to assist wherever possible.

## 1400 Scope

This AMS Plan, by its nature, is very broad in scope, encompassing the whole of the maritime domain within a given COTP zone, and absorbing the individual assessments and planning efforts of facilities and vessels operating within that zone. The scope of this AMS Plan was determined by evaluating the waterways, facilities, vessels, and adjacent areas that may be involved in, or affected by, a TSI in its zone.

The plans required by 33 CFR Parts 104, 105, and 106 provide the foundation of this overarching AMS Plan. However, this AMS Plan extends beyond the required facility and vessel plans in that it seeks to develop strategies to reduce the vulnerabilities of the weakest elements of the port including those vessels, facilities and infrastructure that are not regulated under 33 CFR Parts 104, 105 and 106. Accordingly, pursuant to Title 33 Code of Federal Regulations part 103.100, this AMS Plan applies to all vessels and facilities located in, on, under, or adjacent to waters subject to the jurisdiction of the United States within the Area of Responsibility outlined in paragraph 1711.

In order to meet the requirements of 33 CFR part 103.404, this plan addresses:

1. Operational and Physical Security Measures implemented by Federal, State, and local governmental agencies in MARSEC One;
2. Operational and Physical Security Measures which must be executed by commercial and private entities in order to protect the port in MARSEC One;
3. Additional Security Measures which governmental agencies, commercial entities, and private citizens must execute without delay when the Coast Guard elevates the Security Level to MARSEC Two and MARSEC Three;
4. The inter-agency coordinating organization required to conduct preventive security operations and to respond to suspicious activities, security breaches, and Transportation Security Incidents;
5. The detailed inter-agency and private/commercial response procedures (doctrine) for suspicious activity reports, security breaches, and Transportation Security Incidents;
6. The details for revising, updating, testing, exercising, and auditing this plan;

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-15
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

7. The measures we will employ to prevent dangerous substances and devices from entering designated restricted areas within the ports;
8. The measures we will employ to prevent people from making unauthorized access into designated restricted areas within the ports;
9. The detailed procedures we have for maintaining and restoring critical port infrastructure in the event of a credible threat or a Transportation Security Incident;
10. The identification of and methods of communication with Company Security Officers; Vessel Security Officers; and Facility Security Officers;
11. The measures we will take to protect the security of information in this plan;
12. The procedures for responding if a vessel security alert system is activated;
13. The procedures for communicating appropriate security information and threat information to the public and to the port community;
14. The jurisdiction of federal, state, indian tribal, and local government agencies and law enforcement agencies;
15. Those facilities otherwise subject to 33 CFR part 105 that the Federal Maritime Security Coordinator has designated as a public access facility, along with the security measures that must be implemented at those areas at the various MARSEC Levels (and who must implement them).

## 1500 Suppositions

The following suppositions provide the foundation for the Coast Guard's approach to its MHS mission and successful implementation of the MTSA. In preparing this plan the Port Security Committees made the following suppositions:

1. A terrorist incident may occur at any time with little or no warning.
2. Each entity directly or indirectly involved with the Marine Transportation System will participate with the JMTX Port Security Committee or Port Canaveral Security Committee to increase awareness, conduct joint security mission planning, and enhance prevention of terrorist acts.
3. The National Oil and Hazardous Material Contingency Plan, Federal Response Plan, County Comprehensive Emergency Management Plans and other response plans will be activated as necessary for the purpose of response and crisis management due to a terrorist incident.
4. Security must be maintained during response and crisis management incidents.
5. Protection of human life and health are the most important consideration in plan development and execution.
6. Ports are very open and may be susceptible a Transportation Security Incident (TSI), which may occur at any time with little or no warning.
7. All port areas are susceptible to air attack.
8. It is in the best interest of the U.S. to increase port security by establishing and improving communications among law enforcement officials responsible for port security.
9. It is in the best interest of the U.S. to have a free flow of interstate and foreign commerce and to ensure the efficient movement of cargo.
10. Maintaining continuity of operations and facilitating commerce in the port area is a critical consideration.
11. The transition from Homeland Security to Homeland Defense (under the Department of Defense's Northern Command) occurs when crisis management requires a level of force or scope of operations outside that of law enforcement. Procedures for executing the shift in Lead Federal Agency from the Coast Guard to NORTHCOM will be developed in the future and referenced in this plan.
12. There will be a competition for security resources as threat levels increase.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-16
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

# 1600 Situation

The complexity, scope, and potential consequences of a terrorist threat or TSI occurring within the MTS requires that there be a coordinated effort between all MTS users and law enforcement agencies. This effort will require open communication, enhanced awareness of potential threats and coordinated procedures for prevention, preparedness, response and recovery. It will require those involved to fully understand their roles in enhancing security. See Appendix 9100 for a discussion of the elements of maritime homeland security.

The Coast Guard and the international maritime community have developed a tiered system of Maritime Security (MARSEC) Levels consistent with the Department of Homeland Security’s Homeland Security Advisory System (HSAS). MARSEC is specifically designed to alert users of the MTS. Through this AMS Plan, the stakeholders of the MTS will take certain actions contingent upon the Coast Guard’s activation of MARSEC Levels and develop unified preparedness strategies to deter and respond to security incidents. See section 3400 for communication in the ports.

This section defines the physical, economic, and geographic situation, and is organized as follows:

- 1610 Physical Characteristics
- 1620 Economic Characteristics
- 1630 Port Maps and Charts
- 1640 Information Characteristics

## 1610 Physical Characteristics

This section outlines the physical maritime characteristics of Northeast and Eastern Central Florida. This section has been adapted and modified from the United States Coast Pilot Volume Four. This section is organized as follows:

- 1611 Northeast and Eastern Central Florida Area
- 1612 St. Marys River and Fernandina, chart 11503, Port ID# 21104, UN Locator Code USFEB
- 1613 St. Johns River and Jacksonville, chart 11486, Port ID# 14152, UN Locator Code USJAX
- 1614 Intracoastal Waterway and Coastline, chart 11488-11481
- 1615 Port Canaveral, chart 11478, Port ID# 12716, UN Locator Code USPCA

The following extract from the Coast Pilot Volume Four illustrates these regions and identifies the detailed nautical charts applicable.

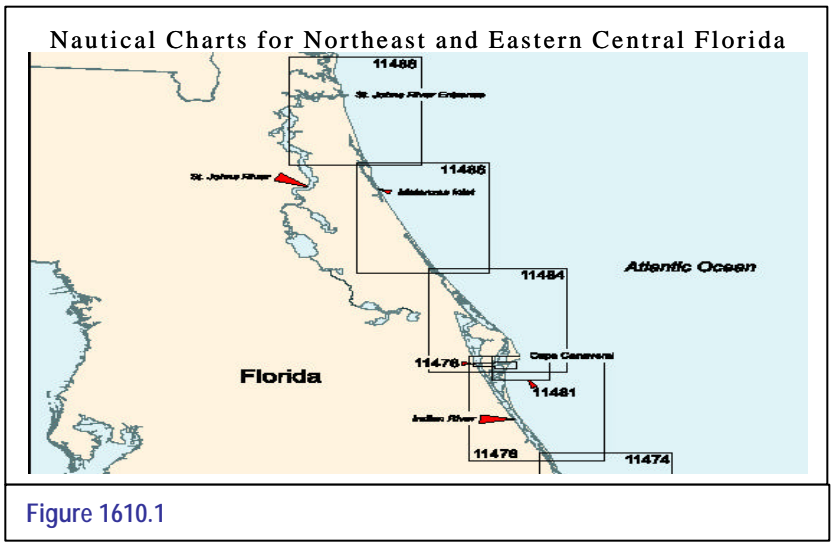


Figure 1610.1

## 1611 Northeast and Eastern Central Florida Area

The Northeast and Eastern Central Florida Area boundaries are defined in Title 33 Code of Federal Regulations part 3.35-20. Specifically, this plan applies in the area bounded by a line that:

- starts at the Georgia coast at 30°.50' N latitude;
- thence proceeds west to 30°.50' N latitude, 82°.15' W longitude;
- thence south to the intersection of the Florida-Georgia boundary at 82°.15' W longitude;
- thence westerly along the Florida-Georgia boundary to 83°.00' W longitude;
- thence southeasterly to 28°.00' N latitude, 81°.30' W longitude;
- thence east to the sea at 28°.00' N latitude.

The offshore boundary:

- starts at the coast at 30°.50' N latitude;
- thence proceeds easterly to the outermost extent of the Exclusive Economic Zone;
- thence southerly along the outermost extent of the EEZ to 28°.00' N latitude;
- thence westerly along 28°.00' N latitude to the coast.



Figure 1611.1

## 1612 St. Mary's River and Fernandina - Chart 11503 – Port ID# 21104 – UN Locator Code USFEB

**St. Mary's River and Cumberland Sound:** The sound is the approach to the city of Fernandina Beach, the city of St. Marys, the Naval Submarine Base in Kings Bay, and an inland passage to St. Andrew Sound through its connection with the Cumberland River. **Fernandina Beach**, the principal city on Cumberland Sound, is on the east bank of the Amelia River, 2 miles (3.21 km) south of the entrance. It is the shipping port for local woodpulp and paper products. Some coastwise and foreign shipping serve the port. A large shrimp boat fleet operates out of Fernandina Beach. **Fort Clinch** (Fig 1612.1), on the south side of the entrance at the north



Figure 1612.1

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-18
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

end of Amelia Island, is a State Park, museum, and recreation area. The old fort and a large red brick building near the inshore end of the south jetty are conspicuous. Camping facilities and a small-craft launching ramp are at the northwest end of the island on the east side of the channel to Fernandina Harbor.

**Channels:** A federal project provides for a depth of 46 feet (14m) in the entrance channel, thence 42 feet (13m) northward through Cumberland Sound to two turning basins of the same depth in Kings Bay about 9.0 and 10.0 miles, respectively, above the outer ends of the jetties. Turning basins are located on the north and south sides of the entrance channel, about 1.7 miles above the jetties, and have project depths of 42 ft. (13m). A channel leads from inside the bar southward in the **Amelia River** with a project depth of 36 feet through the turning basin; thence 28 feet (8m) to a turning basin off the Rayonier Wharf, about 5.8 miles above the jetties.

The entrance to Cumberland Sound is between two stone jetties. The jetties are in very poor condition with both almost entirely submerged at mean high water. The north jetty is marked off its outer end by a lighted buoy and the south jetty is marked off its outer end by an unlighted buoy. Both jetties are marked on their outer sides by unlighted buoys, and on the inner sides by daybeacons. Currents are strong off the ends of the jetties. The natural channel between the jetties is subject to frequent change. St. Mary's Approach Lighted Buoy STM, commonly referred to as the St. Marys sea buoy, (30°40'48"N, 81°11'42"W) is 10.9 miles eastward of St. Mary's Entrance. The channel through the bar and the channels inside the sound are marked with lighted ranges, lights, and lighted buoys. Fishing vessels going northward out of the sound use the natural channel off the end of the north jetty marked by a buoy.

**Anchorage:** Vessels anchor outside St. Marys Entrance about 1 mile northward of the approach range in about 5 to 9 fathoms, sand and mud bottom with good holding ground. Inside the entrance there is fair anchorage along the sides of the channels in Cumberland Sound and in the Amelia River according to draft.

**Tides and currents:** The mean range of tide is 5.8 feet at the entrance and 6 feet at Fernandina Beach. The tidal currents at the entrance have considerable velocity and are dangerous at times, especially on the flood which generally sets northwestward and on the ebb which sets southeastward except during northeast winds when there is a strong southerly set off the end of the jetties on both tides. This set sometimes attains a velocity exceeding 5 knots. Maximum current velocities are reported to be 2.0 to 3.9 knots in St. Mary's Entrance and 1.0 to 2.5 knots in the Cumberland Sound channel. Freshets in the St. Marys River may cause the ebb to run 7 or 8 hours.

**Weather, Cumberland Sound and vicinity:** The climate features short, mild winters and warm, humid summers with fog likely on cool, clear winter mornings. About 50 inches (1270 mm) of rain falls on some 70 days annually. Much of the precipitation occurs in showers or thunderstorms from June through September. Temperatures climb above 90°F (32.2°C) on about 55 days and drop to 32°F (0°C) or below on just 10 days, on the average. By far the biggest threat to this pleasant climate is hurricanes, which are most likely from June through November. While the area is vulnerable to this threat, direct landfalling hurricanes are rare, and those that pass offshore cause relatively minor damage. The most dangerous tropical cyclones are those that cross the coast from the east through southeast and those that approach from the south through southwest. During hurricane Dora (September 1964) winds of 85 knots or more extended from St. Augustine to Fernandina Beach. Unusually high tides were generated by prolonged onshore winds. The Amelia River tide gauge recorded readings to 10 feet (3 m) above normal. From experience it can be suggested that, when winds reach 50 knots or more and tides surge to 8 to 10 feet (2 to 3 m) above normal at the Amelia River gauge, there is a likelihood of sudden shoaling in the St. Marys River entrance. A severe threat to shipping should be anticipated when a hurricane is expected to make landfall within 90 miles (167 km) south, or 30 miles (56 km) north, or when a severe tropical storm (50-63 knots) is expected to make landfall within 60 miles (111 km) south, or 20 miles (37 km) north of the St. Marys River entrance.

**Wharves:** The Ocean Highway and Port Authority of Nassau County owns one major commercial pier on the Amelia River, the Port of Fernandina. There are two privately owned facilities for deep-draft vessels at Fernandina Beach. Both have highway and rail connections. Depths alongside are reported depths. There

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-19
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



are numerous smaller facilities along the waterfront which are used for the receipt of seafood and servicing of commercial fishing vessels and small craft.

**Container Corporation of America Wharf (Fig 1612.2):** (30°40'58"N, 81°27'37"W): east side of Amelia River about 1.5 miles above the channel entrance; offshore wharf with 365 feet of berthing space with dolphins; 29 feet alongside; deck height, 14 feet; hose handling equipment; untreated water available; handles fuel oil for plant consumption.



Figure 1612.2

**The Port of Fernandina:** east side of Amelia River about 1.75 miles above the channel entrance; marginal wharf with 1200-foot face; 36 feet reported alongside; deck height, 12 feet; transit sheds with 200,000 square feet of storage; 12 acres of open storage. Two container cranes, one whirley crane are operated by **Nassau Terminals**.(Fig 1612.3)



Figure 1612.3

**Rayonier Wharf (Fig 1612.4):** east side of Amelia River, about 1.3 miles southward of the Container Corporation of America Wharf; marginal wharf with 400-foot face, 500 feet with dolphins; 27 to 30 feet alongside; deck height, 14 feet; electrical shore power connections; untreated water available; handles caustic soda, and fuel oil for plant consumption.



Figure 1612.4

**Repairs:** There are no drydocking or major repair facilities for oceangoing vessels at Fernandina Beach; the nearest such facilities are at Jacksonville. Machine, welding, and electrical shops off the waterfront can make limited above the waterline repairs. The larger of two marine railways is on the east side of Amelia River, about 0.6 mile northward of Rayonier Wharf; vessels up to 130 feet in length and 12-foot draft can be handled for hull, engine, and electrical repairs.

**Transportation:** Fernandina Beach is served by State Route A1A, CSX Railroad (freight service only), and an airport. There are bus connections to Jacksonville where there are passenger rail connections. Ferryboat service is available to Cumberland Island.

VERSION DATE	V_1.1 26 May 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-20
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**Small-craft facilities:** The **Municipal Marina (Fig 1612.5)** is on the east side of the Amelia River, about 2.3 miles southward of the channel entrance and 0.5 mile northward of Rayonier Wharf. In May 1983, depths of 4 feet were reported in the slips, with depths of 8 feet reported alongside the pier facing the river. Berthage with electricity, gasoline, diesel fuel, water, ice, marine supplies, and a launching ramp are available. A 4-ton fixed lift and a marine railway that can handle craft to 75 feet are available; hull, engine, and electrical repairs can be made. Gasoline, diesel fuel, and water can also be obtained at the two fuel piers, northward and southward of the marina.



Figure 1612.5

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-21
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1613 St. Johns River and Jacksonville – Chart 11488

### Port ID# 14152 – UN Locator Code USJAX

**St. Johns River**, the largest in eastern Florida, is about 248 miles long and is an unusual major river in that it flows from south to north over most of its length. It rises in the St. Johns Marshes near the Atlantic coast below latitude 28°00'N, flows in a northerly direction, and empties into the ocean north of St. Johns River Light in latitude 30°24'N. The river is the approach to the city of Jacksonville and a number of towns near its shores. Some of these places are winter resorts while others are centers of farming districts and citrus groves. Deep-draft vessels go as far as just below the Main Street (John T. Alsop) Bridge. Southward of the Jacksonville bridges, commercial traffic is light and consists almost entirely of oil barges. Many pleasure craft navigate this part of the river, usually going only as far as Sanford, though small boats have navigated the river as far as Lake Washington, 188 miles south of Jacksonville. The Intracoastal Waterway crosses the St. Johns River at nearly right angles about 5 miles above the mouth, at about 30°23.1'N, 81°27.8'W.

**Jacksonville** has expanded by consolidation to include most of Duval County and is now the largest city in the United States in terms of area; it extends along the St. Johns River from the ocean to the town of Orange Park on the west side of the river and to Julington Creek on the east side. Most of the marine terminals are on the west side of the river about 21 miles above the entrance, just above the point where the river first turns southward. The deepwater port is the largest on the east coast of Florida. It is a major southeastern bulk-handling, distribution, and railroad center. Both general and bulk cargoes are handled, and Jacksonville is a leading southeastern container port. The principal exports are paper products, phosphate rock, fertilizers, chemicals, citrus products, naval stores, tallow, clay, scrap metal, feed, and general cargo. The principal imports are petroleum products, coffee, iron and steel products, limestone, pulpwood, cement, automobiles, lumber, chemicals, alcoholic beverages, and general cargo.

**Anchorage:** Vessels waiting outside the entrance to St. Johns River can anchor in depths of 36 to 50 feet north-northeastward of the jetties if wind and sea permit. Anchorage south of the south jetty is not recommended because of the heavy shrimp boat activity in that area. Merchant ships are normally anchored either in the area off Talleyrand Docks and Terminals, locally termed the lower anchorage, or in the area off Commodore Point, known as the upper anchorage. Though these are the only practical anchorages available, the holding ground is marginal and both anchorages are somewhat constricted. See 33CFR110.183.

**Tides and currents:** The mean range of tide is 4.9 feet at St. Johns River entrance and about 1.2 feet at the railroad bridge at Jacksonville. From Jacksonville to Palatka the mean range of tide is about 1 foot. At low-water stages, tidal action is felt to Lake George. The tidal currents are strong in the St. Johns River as far as Jacksonville. The currents at the entrance between the jetties require special attention.

**Weather, Jacksonville and vicinity:** Jacksonville is near the northern boundary of the trade winds in summer. Winds off the water produce a maritime influence that tempers the heat of summer and cold of winter. Winter storms and severe cold waves often remain north of the area. Occasionally a “nor-easter” will skirt the Florida coast bringing 15- to 30-knot winds, low stratus clouds and drizzle. These are most likely in late summer and fall. This area lies within the hurricane belt although hurricane force winds are rare, since most storms either remain offshore or have tracked inland and weakened. The average high temperature in Jacksonville is 79°F (26.1°C) and the average low is 59°F (15°C). By a fraction of a degree, July is the warmest month with an average high of 92°F (33.3°C) and an average low of 73°F (22.8°C). January is the coolest month with an average high of 65°F (18.3°C) and an average low of 43°F (6.1°C). May through August have recorded temperatures in excess of 100°F (37.8°C) and the all-time maximum temperature is 103°F (39.4°C) recorded in June 1950, June 1954, and again in July 1981. Below freezing temperatures have been recorded from November through March and the record minimum is 7°F (-13.9°C) recorded in January 1985. On average, 83 days each year has a maximum temperature of 90°F (32.2°C) or greater while only 15 days can be expected to have minimums of 32°F (0°C) or below. Over one-third of the annual average rainfall of 53 inches (1346.2 mm) falls during the summer months of June, July, and

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-22
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



August. September is the wettest month averaging 7.67 inches (194.8 mm) and November is the driest month averaging about 2 inches (50.8 mm). Most of the summer rainfall is compliments of convective activity or precipitation of a tropical origin. Snowfall is almost unheard of however small amounts have fallen in each month, December through March. The greatest 24-hour snowfall was 1.5 inches (38.1 mm) falling in February 1958.

On average the Jacksonville area is threatened by tropical cyclones (within 50 nm (93 km) once or twice each year. While this may occur in any month it is most likely from June through October, with a peak in September and November. Most storms cross over the Florida peninsula and weaken. The Port of Jacksonville and Mayport Basin are not considered hurricane havens since surrounding low topography does not provide an adequate windbreak. See Captain of the Port Policy letter 04-02 dated May 30, 2002. Special care should be taken with storms approaching from the southeast. Since 1842, 69 tropical cyclones have come within 50 miles (93 km) of Jacksonville; 21 of those storms have done so since 1950.

In general, prevailing winds are northeasterly in fall and winter and southwesterly in spring and summer, although afternoon sea breezes often bring winds off the water in these latter seasons. Windspeeds are often highest from September through April when they exceed 17 knots about 3 to 8 percent of the time. Local climatic variations are most noticeable in the heat of summer. Along the beach, on 20 to 30 days annually, temperatures reach the 90's (°F) compared to 70 to 80 days near the city. Fog is mainly a wintertime phenomena, rolling in with any easterly wind but often remaining across the entrance when it has cleared elsewhere. In calm weather, smog from fertilizer and paper plants often obscures the channel above Dames Point. Radiation-type fog, which may occur near the city, usually burns off by noon. On the average, there are 25 to 35 days annually, when visibilities drop below 0.5 mile; November through February are the most likely months. Summer showers and thunderstorms are responsible for much of the precipitation in the area. Thunderstorms are most likely during June, July, and August, when they occur on about 10 to 16 days per month. See NOAA Weather Buoy, [www.ndbc.noaa.gov](http://www.ndbc.noaa.gov).

**Channels (Fig 1613.1):** Along the coast from Charleston to Jacksonville, the course between the outer lighted whistle buoys (sea buoys) is from 10 to 15 miles offshore.

Approaching from the southward, vessels clear Hetzel Shoal before shaping a course for St. Johns River entrance. A Federal project provides for a channel 40 feet deep from the ocean to buoy 59, thence 38 feet deep to a point 2.1 miles north of the Mathews Bridge, thence 34 to 38 feet deep to

Commodore Point via Terminal Channel. The main channel is maintained at or near project depths. A lighted buoy with a racon is about 3 miles off the entrance to the river. The entrance channel, between two converging rubblestone jetties, and the channel in the river are marked by lighted and unlighted buoys, lights, and lighted ranges. Overhead power cables with a clearance of 175 feet cross the river about 9 miles above the entrance at Blount Island.

**Mayport Basin (Fig 1613.2)** is on the south side of the St. Johns River just inside the entrance jetties and westward of St. Johns Point. A deep channel leads along the inshore end of the south jetty to the basin. It is marked by a 255° lighted range, lights, and lighted and unlighted buoys. The waters of the turning basin are within a prohibited area of the U.S. Naval Station Reservation; commercial and pleasure vessels are prohibited from entering except in cases of extreme emergency. See 33CFR 334.500.

**Mayport** is a town on the south bank of St. Johns River, 3 miles inside the entrance jetties. It has a ferry

[Reserved photo channels Figure 1613.1]



Figure 1613.2

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-23
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

connection with the town of Fort George Island across the river. The wharves at Mayport are private and are used by fishing vessels. A Coast Guard base is at the southerly end of the waterfront. There is a marina and a yacht basin with reported depths of about 10 feet. See U.S. Army Corps of Engineers Port Series No.15, Port ID 64-77.

**The Intra-Coastal Waterway (Fig 1613.3)** crosses the St. Johns River 5.3 miles from the entrance through Sisters Creek on the north and Pablo Creek on the south. A shipbuilding and drydock company, Atlantic Marine, (USACE Port Series No.15, Port ID 4-7) is on the north side of the river and on the east side of Sisters Creek. The firm builds steel-hulled tugs and fishing vessels and does all kinds of repair work on commercial and Government vessels. There is a 4,000-ton marine railway, several mobile cranes, a floating dry-dock, complete shop facilities, and berths for vessels of up to 585 feet. The marine railway is on the St. Johns side of the yard, while the construction work is done on the Sisters Creek side.



Figure 1613.3

**Blount Island (Fig 1613.4)**, low and sandy with fringing marshes, is on the north side of the St. Johns River about 9 miles above the entrance. The Jacksonville Port Authority terminal near the southwestern tip of the island, and Gate Maritime Terminal in Back River (Gate Maritime Slipway) at the southeastern tip of the island have been described under **Wharves** for the Port of Jacksonville. Blount Island Channel, a cutoff bend of the St. Johns River, extends from the main river channel around the northern side of Blount Island and rejoins the main channel at the southwestern tip of the island. The channel is practically divided near its midpoint by four low fixed bridges with clearances of 18 feet horizontally and 5 feet vertically. Overhead power cables, with clearances of 175 feet, are on both sides of the southwestern-most highway bridge. The Federal project depth for the channel is 38 feet, but the controlling depth is usually considerably less than project depth. Two deep-draft private wharves are on the marked western leg of Blount Island.



Figure 1613.4

**The Dames Point Bridge (Fig 1613.5)** with a clearance of 169 feet crosses St. Johns River just above Blount Island at Dames Point. Broward River, on the north side and 13 miles from the entrance to St. Johns River, has depths of 1 to 3 feet to Cedar Heights. The Heckscher Drive (State Route 105) highway bridge at the mouth has a 40-foot bascule span with a clearance of 13 feet. Overhead power cables at the bridge have a least clearance of 34 feet. The offshore wharf and shore facilities of a U.S. Navy Fuel Depot are 1.2 miles southwestward of Drummond Point on the northwest side of the St. Johns River, just below the mouth of the Trout River. The wharf has a 351-foot face, 660 feet of berthing space with dolphins, 38 feet alongside, and a deck height of 11 feet. Pipelines extend from the wharf to storage tanks onshore. The fuel depot is in a restricted area. See 33CFR334.510.



Figure 1613.5

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-24
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**Trout River (Fig 1613.6)**, north of downtown Jacksonville, has depths of 7 feet to the mouth of Ribault River and 3 feet to the highway bridge 4.5 miles above the mouth. The entrance is marked by daybeacons. A small repair yard is on the east side of a small cove on the south side of the river about 0.4 mile above the entrance. The yard has berths, electricity, water, two 6-ton lifts, and a marine railway that can handle craft up to 85 feet long or 200 tons. Depths of 8 feet are reported in the approach and alongside.



**The Main Street (U.S. Route 17) Highway Bridge (Fig 1613.7)** 0.9 mile above the entrance has a fixed span with a clearance of 29 feet. The highway bridge, adjacent to the westward, except for the channel span, remains as a fishing pier. The overhead power cable at the bridge has a clearance of 38 feet. The Seaboard System Railroad (SCL) bridge just upstream as a swing span with a channel width of 46 feet and a clearance of 2 feet. The overhead power cable, 0.5 mile above the bridge, has a clearance of 45 feet. A marina on the south side, just east of the Main Street bridge, has berths, electricity, gasoline, diesel fuel, water, and a launching ramp. The Interstate 95 highway bridge, 2 miles above the mouth, has a fixed span with a clearance of 29 feet at the center. State Route 115 highway bridge, 4.5 miles above the mouth, has a 40-foot fixed span with a clearance of 18 feet. The overhead power cable just westward of the bridge has a clearance of 45 feet. Groups of pilings, sunken wrecks, and barges are near the shores of Trout River. There are numerous private piers and landings on the river. The Jacksonville City Zoo is on the north side of the river downstream of the first bridge.



**Bridges (Fig 1613.8):** Seven bridges cross the St. Johns River at downtown Jacksonville. The Dames Point Bridge with a clearance of 169 feet crosses the river just above Blount Island at Dames Point. The fixed Matthews highway bridge, 0.5 mile north of Commodore Point, has a clearance of 152 feet across the main (Terminal) channel and 86 feet at the center of the span across Arlington Channel. At Commodore Point, the Hart suspension bridge has a clearance of 135 feet, with 141 feet at the center. Main Street (Alsop) highway bridge, the first of four bridges at Hendricks Point, has a vertical-lift span with clearances of 40 feet down and 135 feet up; the second, Acosta highway bridge, 0.3 mile upstream from the Main Street bridge, has a fixed span with a clearance of 75 feet; the third, the (FEC) Railway Co. bridge adjacent to the Acosta bridge, has a bascule span with a clearance of 5 feet; the fourth, the Fuller Warren highway bridge, has a fixed span with a clearance of 65 feet at the center.



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-25
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**The Ortega River (Fig 1613.9)** is about 2 miles south of Fuller Warren Bridge (30°18.9'N., 81°40.3'W.) on the west side of the St. Johns River. It is the major yachting center in the Jacksonville area. The mouth of the river is marked by a light. In May 1983, the reported controlling depth was 6 feet across the bar at the entrance, thence 7 feet to the railroad bridge, thence 5½ feet for a distance of 1.4 miles above the second highway bridge. The Grand Avenue (State Route

211) highway bridge, at the entrance to Ortega River connecting Ortega and St. Johns Park has a bascule span with a clearance of 9 feet. The Roosevelt Boulevard (U.S. Route 17) highway bridge, 0.7 mile upstream, has dual fixed spans each with a clearance of 45 feet. The northern 180-foot section of the former highway bascule bridge immediately westward remains as a fishing pier. An overhead power cable with a clearance of 65 feet is at the fishing pier. The Seaboard System Railroad (SCL) bridge immediately westward of the fishing pier has a 40-foot bascule span with a clearance of 2 feet. The Timquana Road highway bridge crossing the river 1.9 miles above the railroad bridge has a fixed span with a clearance of 20 feet.

[Reserved ortega bridges photo Fig 1613.9)]

**Jacksonville Naval Air Station (Fig 1613.10)** extends along the west side of the St. Johns River about 0.7 mile northwestward of and 2.5 miles south-southwestward of Piney Point. A large pier is south of Piney Point. In April 1982, the dredged channel leading to the pier had a controlling depth of 14 feet to the outer end of the pier except for shoaling to 13 feet along the northeast edge of the basin, thence 16 feet north and 11 feet south of the pier. Another dredged channel leads to a small basin and marina at the station about 2.4 miles southward of Piney Point. In 1978, the controlling depth was 9 feet in the channel and 6 feet in the basin except for shoaling to 3 feet at the west end. See 33CFR 165.

[Reserved nas jax photo Fig 1613.10]

The twin fixed spans of **Highway 295 Bridge (Fig 1613.11)** (Buckman Bridge), with clearances of 65 feet cross the St. Johns River just below the Naval Air Station, 2.5 miles southward of Piney Point.

[Reserved buckman bridge photo Fig 1613.11]

**Doctors Inlet (Fig 1613.12)**, 10.5 miles southward of Fuller Warren Bridge, is the entrance to Doctors Lake from the St. Johns River. In May 1983, the inlet had a reported controlling depth of 12 feet, thence general depths of 7 to 12 feet to the head of the lake. Because of extensive shoals on both sides of the inlet, midchannel courses must be steered from abeam of Light 10 until through the inlet. The lake is an excellent fishing ground for sportsmen and haven for small boats in stormy weather. U.S. Route 17 fixed highway bridge with a clearance of 37 feet crosses the mouth of Doctors Inlet.

[Reserved doctors inlet photo Fig 1613.12]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-26
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



**Julington Creek (Fig 1613.13)**, 13 miles south of Fuller Warren Bridge on the east bank, had a reported controlling depth of 5 feet in May 1983, to State Route 13 highway bridge about a mile inside the entrance, thence 4½ feet for another 1.3 miles. The highway bridge has a 44-foot fixed span with a clearance of 15 feet. An overhead power cable with a clearance of 40 feet crosses the creek at the bridge on the east side. The southern city limit of Jacksonville follows the north side of Julington Creek.

[Reserved julington creek photo  
Figure 1613.13]

**Green Cove Springs** has a port and airport located at the Green Cove Springs Navy Base which was closed in the 1960's.

**Wharves:** Of the 23 principal piers and wharves described for the port, many are operated by the Jacksonville Port Authority; others are privately owned and operated. Most of the terminals have excellent highway connections. Three switching railroads connect the terminals and the three major railroads serving Jacksonville. General cargo at the port is usually handled by port cranes, and equipment is available for all lifts.

**Celotex Corp. Dock (Fig 1613.14):** west side of Blount Island Channel (old river channel), 0.35 mile northward of the southwest tip of Blount Island; offshore wharf with 20-foot face, 536-foot berth with dolphins; deck height, 10 feet; adjustable receiving hopper on wharf connected by conveyor to open storage area.



Figure 1613.14

**Gate Maritime Terminal:** five berths, capable of berthing vessels in excess of 1,000 feet along both sides of Back River (Gate Maritime Slipway), at the southeast end of Blount Island; maximum draft permitted alongside is 37ft (berths 1-2) and 38 ft (berths 3-4); deck height, 10 feet; one 40-ton crane; water and electrical connections; receipt and shipment of miscellaneous bulk materials, notably gypsum and lime rock, mooring vessels and harbor tugs, and handling heavy-lift items and military cargo; used by commercial and government vessels; owned and operated by Gate Maritime Properties, Inc. See USACE Port Series No.15, Port ID 8-12.



Figure 1613.15

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-27
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**St. Johns River Coal Terminal (Fig 1613.16):** on main St. John River channel east of Jacksonville Port Authority berths, 10 miles above St. Johns River entrance; 808-foot bulkhead wharf; 38 feet alongside; deck height 9 feet 45-ton clamshell bucket unloader, unloads coal on to a conveyor system which transports coals to a coal-fired generation station 3.5 miles inland, unloading rate 750-1500 tons per hour; operated by St. Johns River Power Park. See USACE Port Series No.15, Port ID 13.



Figure 1613.16

**Blount Island Port ID# 27239 UN Locator Code USJAX (Fig 1613.17):** has seven berths on the main St. Johns River channel on the west part of Blount Island, 10 miles above St. Johns River entrance; 5,250-foot bulkhead wharf; 38 feet alongside; deck height, 9 feet; cranes to 45 tons; handles containerized, conventional, and roll-on roll-off general cargo, automobiles, steel products, kraft paper, and lineboard rolls; operated by Jacksonville Port Authority. A 600-foot dock on the west side of Blount Island is operated by the port and used for the loading and unloading of automobiles.



Figure 1613.17

**North Side Generating Station Wharf (Fig 1613.18):** northwestern side of Blount Island Channel, 1.15 miles northeastward of Kaiser Gypsum Co. Wharf and 0.2 mile southwestward of the Blount Island highway bridge; offshore wharf with 60-foot face, 700 feet with mooring dolphins; 36 feet alongside; deck height, 13½ feet; fuel oil for plant consumption; operated by Jacksonville Electric Authority. See USACE Port Series No.15, Port ID 19.



Figure 1613.18

**Dames Point Aggregate Docks: (reserved)**

**Dames Point Cruise Terminals: (reserved)**

**Ed Austin Terminal: (reserved)**

**Amerada Hess Corp., Jacksonville Terminal Wharf (Fig 1613.19):** north side of St. Johns River at mouth of Broward River, 0.3 mile east-northeastward of Drummond Point; offshore wharf with 300-foot face, 800 feet with mooring dolphins; 38 feet alongside; deck height, 12 feet; handles petroleum products, Bunker C, and occasional loading of harbor bunkering barges. See USACE Port Series No.15, Port ID 22.



Figure 1613.19

**Drummond Point Terminal (Fig 1613.20):** extending from Drummond Point; offshore wharf with 143-foot face, 1,000-foot berth with dolphins; 38 feet alongside; deck height, 12 feet; hose-handling derrick; handles petroleum products and loading harbor bunkering-barges; operated by BP. See USACE Port Series No.15, Port ID 23.



Figure 1613.20

**U.S. Gypsum Co. Pier (Fig 1613.21):** just south of Trout River entrance on west side of St. Johns River at 30°23'01.5"N, 81°37'55.0"W; pier 616 feet long and 42 feet wide, berthing only along south side, usable space 455 feet with dolphins; 33 feet alongside; deck height, 6 feet; self-unloading vessels discharge into a hopper served by a conveyor system, which extends full length of pier to an open storage area ashore handles gypsum rock. See USACE Port Series No.15, Port ID 26.

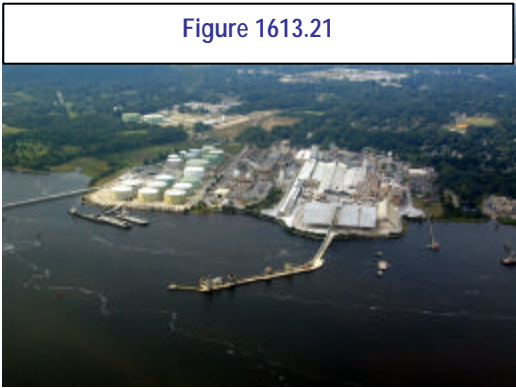


Figure 1613.21

**ST Services Wharf (Fig 1613.22):** 0.34 mile southward of U.S. Gypsum Co. Pier, west side of river; offshore wharf with 80-foot face, 1,000 feet with mooring dolphins; 38 feet alongside; deck height, 12 feet; handles petroleum products. See USACE Port Series No.15, Port ID 28-29.



Figure 1613.22

**PCS Phosphate (Fig 1613.23):** on south side of entrance to Long Branch Creek, offshore wharf consisting of a line of dolphins connected by catwalks, 800-foot berth; 38 alongside; deck height, 10 feet; 2 loading towers, each with a loading rate of 3,000 long tons per hour; towers are served by conveyor from phosphate storage silos, handles phosphate rock, phosphoric acid, and phosphatic products. The facility is closed. See USACE Port Series No.15, Port ID 30.



Figure 1613.23

**Alton Box Board Co. Fuel Dock (Fig 1613.24):** 30°22'03"N, 81°37'31"W; offshore wharf with mooring dolphins in line with face, 51-foot face, 250-foot berth with dolphins; 24 feet alongside; deck height, 10 feet; hose-handling derrick; pipeline connects wharf and storage tanks; handles fuel oil for plant consumption. Facility closed and entered caretaker status in 2003. See USACE Port Series No.15, Port ID 31.

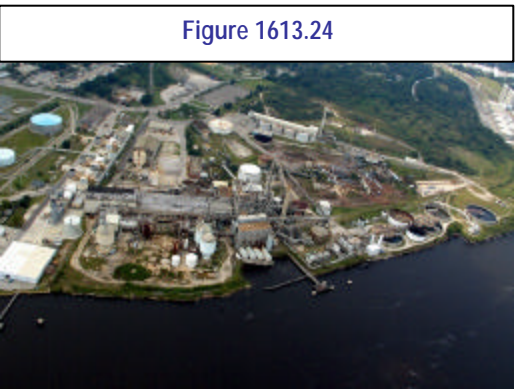


Figure 1613.24



**J. Dillon Kennedy Generating Station Wharf (Fig 1613.25):** 30°21'53"N, 81°37'22"W; offshore wharf with 101-foot face 220-foot berth with two dolphins; 28 feet alongside; deck height, 10 feet; handles fuel oil for plant consumption; operated by Jacksonville Electric Authority. See USACE Port Series No.15, Port ID 32.

Figure 1613.25



**Coastal Fuels Marketing, Inc. Terminal Wharf (Fig 1613.26):** west side of river, 0.29 mile southeastward of J. Dillon Kennedy Generating Station Wharf; offshore wharf with 140-foot face, 750-foot berth with dolphins; 32 feet alongside; deck height, 13 feet; hose-handling derrick; handles asphalt products. See USACE Port Series No.15, Port ID 33.

Figure 1613.26



**Chevron Tanker Dock (Fig 1613.27):** west side of river, 0.16 mile south of Belcher Oil Co. Terminal Wharf; 50-foot face, 280-foot berth with dolphins; 36 feet alongside; deck height, 12 feet; hose-handling derricks; handles petroleum products; operated by Chevron USA, Inc. See USACE Port Series No.15, Port ID 34.

Figure 1613.27



**Talleyrand Marine Terminal (Fig 1613.28):** west side of river at 30°20'42" N, 81°37'20" W; approximately 21 miles from the entrance to the St. John's River; 173 acres of lighted and secured cargo storage area; eight berths providing 4,800 feet of continuous berthing space; five container cranes, two rubber tired gantry cranes, one 100-ton multi-purpose whirly crane, tanker discharge facilities and three 40-ton container stackers; apron width 80 feet; depth alongside MLW: 36 feet; deck height above MSL: 7 feet; handles

Figure 1613.28



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-31
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

containerized cargo, general cargo, refrigerated and frozen cargo, automobiles, molasses, caustic soda, lumber, steel products, chemicals and lignin sultanate. Talleyrand Terminal Railroad, a rail switching contractor to Jaxport, provides on-dock switching for CSX, Norfolk Southern and Florida East Coast Railroad. Municipal Docks Railway connects the terminal with all trunk carriers serving the port. See USACE Port Series No.15, Port ID 36-38.

**Jacksonville Port Authority, 8th Street**

**Terminal (Fig 1613.29):** west side of river at 30°20'42"N, 81°37'20"W; 700-foot bulkhead wharf; 36 feet alongside; deck height, 9 feet; handles automobiles; operated by Joyserv Co. Ltd. See USACE Port Series No.15, Port ID 39.

Figure 1613.29



**Crowley Liner Services Trumbull Asphalt**

**Dock (Fig 1613.30):** west side of river 0.7 mile north of the Matthews bridge; 425-foot face; 26 feet alongside; deck height 9 feet; receipt of asphalt. See USACE Port Series No.15, Port ID 40.

Figure 1613.30



**Crowley TMT Barge Dock (Fig 1613.30):**

west side of the river immediately south of the CLS Trumbull Asphalt Dock and 0.5 mile north of the Matthews bridge; 3 mooring dolphins extend out in a line from the West bank 430 feet; 260-foot face; 23 feet alongside; deck height, 9 feet; 3 deck roll-on/roll-off ramp; handles containerized ro-ro general cargo, automobiles, and heavy-lift items. See USACE Port Series No.15, Port ID 41.

**Commodore's Point Terminal Wharf – Port ID# 27271, UN Locator Code USJAX (Fig 1613.31):**

West side of the river at Commodore Point; 700-foot face; 27 feet alongside; deck height, 5½ feet; handles conventional general cargo, petroleum products, chemicals bulk cement, bananas, and fertilizer; various operators. See USACE Port Series No.15, Port ID 44-46.



Figure 1613.31

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-32
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**The Landing (Fig 1613.32): (reserved)**  
See USACE Port Series No.15, Port ID 42,43,48-51.



**Adam's Mark (Fig 1613.33): (reserved)**  
See USACE Port Series No.15, Port ID 57.



**Repairs:** A shipyard is on the river at the junction with Sisters Creek (Intra-Coastal Waterway), see USACE Port Book Series No.15, Port ID 4-7, and has a 4,000-ton marine railway and a floating drydock. A shipyard on the west bank of the river at **Commodore Point** has a floating drydock with a 2,800-ton lift capacity for vessels up to 389 feet in length and 3 wet berths for vessels up to 700 feet in length and 25-foot draft with complete shipyard facilities available. See USACE Port Series No.15, Port ID 46-47. In addition to the shipyards, Jacksonville has all types of specialized marine manufacturing, sales, and repair firms which handle such items as electronic equipment, electric motors and other components, ventilation and air conditioning systems, shafts and propellers, etc.

**Transportation:** The port is served by three railroads - CSX, Norfolk Southern and Florida East Coast Railway Company. The Jacksonville Port Authority contracts Talleyrand Terminal Railroad to provide rail switching services to its tenants at the Talleyrand Marine Terminal. CSX provides switching services to tenants of the Blount Island Marine Terminal. Excellent highways reach the city, and there is an expressway system providing rapid transportation within the city; the primary highways leading from Jacksonville are Interstate Highways 10 and 95, and U.S. Routes 1,17 and 90. Jacksonville International Airport, is approximately 10 miles north of the city center and is served by six airlines. Both passenger and air freight service is available. There are also three general-aviation airports in the city. Numerous steamship lines connect with most of the principal foreign and domestic ports. Barge service is available for the Intracoastal Waterway, coastwise, and up the St. Johns River as far as Sanford.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-33
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1614 Intracoastal Waterway and Coastline Charts 11488 & 11481

**The Intra-Coastal Waterway** enters Cumberland Sound from the Cumberland River and continues through the Amelia River on the south. **Beach Creek** extends northward into Cumberland Island from a point just inside the entrance to Cumberland Sound. In February 1978, 2 feet was reported at the entrance, and the creek dried about 0.2 mile below Dungeness. **Kings Bay (Figure 1614.1)** is the northwesterly part of Cumberland Sound, about 5 miles above its southerly entrance. The Naval Submarine Base here has a drydock and a 2,000-foot wharf with depths of 40 feet reported alongside in May 1983; deck height is about 14 feet. A rail spur line connects the terminal with the Seaboard System Railroad; two transit sheds and two 10-ton mobile hoists are available. See 33CFR 165.731. The facility is owned by the U.S. Government. A **regulated navigation area** has been established in Cumberland Sound in the vicinity of Kings Bay. See 33CFR165.730.

[Reserved photo kings bay Fig 1614.1]

in

**St. Marys River (Fig 1614.2)**, the principal tributary of Cumberland Sound, enters from westward, and is a portion of the boundary between Georgia and Florida. It is used primarily by shrimp fishermen and tugs towing fuel oil as far as the city of St. Marys. The controlling depth in the channel to St. Marys is about 14 feet. Above St. Marys a vessel with a draft of 10 feet or less should have little difficulty going as far as Kings Ferry, which is 32 miles above the mouth. The river is very crooked, and some of the turns are sharp. Unpredictable currents have been reported in the entrance to the river, at the junctions with Jolly and North Rivers, and along the piers at St. Marys. The mean range of tide is 5.8 feet at the entrance, 6 feet at St. Marys, and 4.8 feet at Crandall, 5 miles above the mouth. The water is fresh above the Seaboard System Railroad bridge, 20 miles above the mouth. The twin fixed spans of U.S. Route I-95 highway bridge with a clearance of 35 feet crosses St. Marys River about 15.2 miles above the mouth. U.S. Route 17 highway bridge at Wilds Landing, 20 miles above the mouth of the river, has a swing span with a clearance of 5 feet. The Seaboard System Railroad bridge just upstream has a swing span with a clearance of 5 feet. Overhead power cables close upstream of the bridge have a least clearance of 55 feet.

[Reserved photo st marys Fig 1614.2)]

The town of **St. Marys** is on the north bank of St. Marys River, 4 miles above the mouth. The larger wharves here are used by fishing boats and have depths of about 13 feet alongside. A U.S. Coast Guard Maritime Safety and Security Team is stationed in St. Marys. Diesel fuel and water are available. However, it is reported that strong currents, the large tidal range, and the exposure to winds refuge in bad weather by anchoring near the pulp mill 1 mile up North River or near the bridges 16 miles above St. Marys on the St. Marys River. **North River** branches from St. Marys River about 2 miles above its mouth. In May 1983, it was reported that a draft of 7 feet could be carried to the pulpmill dock up the river. **Bells River** branches from St. Marys River about 1.5 miles above the town of St. Marys. It flows in an easterly direction to its junction with the Amelia River at Fernandina Beach. In May 1983, the reported controlling depth was about 4 feet. **Chester**, a town on the river, has a number of small docks which were reported in ruins in May 1983. **Jolly River** branches eastward from Bells River about 6 miles above its mouth, and empties into Cumberland Sound at the mouth of St. Marys River. In May 1983, the reported controlling depth was about 7 feet. **Lanceford Creek** branches from Amelia River west of Fernandina Beach. The southern entrance where it joins Amelia River dries clear across. In May 1983, it was reported that with local knowledge a depth of about 7 feet could be carried from the creek's eastern entrance, junction with Bells River, to the docks at **Black Rock**. The creek widens off the docks into tidal flats which bare at low water.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-34
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



Small boats cross from the creek to Amelia River at high tide through **Soap Creek**, which passes through numerous mud flats and oyster beds that bare at low tide.

From St. Marys Entrance to St. Johns River the coast is formed by the shores of Amelia, Talbot, Little Talbot, and Fort George Islands. **Amelia Island (Fig 1614.3)** is nearly north and south, with a length of about 12 miles and a width varying from 1 to 2.5 miles. The island is low and gently undulating with heavy woods along the shore. In front of the woods a range of sand dunes, partly covered with coarse grass and scrub, backs the broad stretch of white sand beach.

[Reserved photo coastline islands Fig 1614.3)]

Several landmarks are prominent along this stretch of the coast. About 3 miles south-southeast of Amelia Island Light is a pier extending 800 feet into the ocean. The western portion of Amelia Island is marshy. Separating the island from the mainland is a broad stretch of marsh through which flow the Amelia and South Amelia Rivers connecting Cumberland Sound and Nassau Sound.

**Nassau Sound** is 10 miles southward of Amelia Island Light and 6 miles northward of St. Johns River. The entrance is obstructed by shifting shoals which extend about 1.5 miles seaward and form a shallow bar. Breakers form across the entire entrance. The mean range of tide in Nassau Sound is 5.4 feet. Route A1A highway toll bridge, 1 mile above the entrance, has a swing span with a clearance of 15 feet. Vertical clearance of the bridge through the bents is about 9 feet. A small-craft launching ramp is on the south side of the bridge. South Amelia River and Nassau River are the principal tributaries of Nassau Sound.

**South Amelia River** enters from the northward and is a portion of the Intra-Coastal Waterway. **Nassau River** enters Nassau Sound from the northwestward. **Nassauville** is a small settlement on the north bank of the river, 7 miles above the entrance to the sound, with private piers adjoining private homes and a fishing camp. Local knowledge is necessary to carry the best water to Nassauville and **Christopher Creek**, where there is a private marine railway which can haul out craft up to 50 feet in an emergency. **Alligator Creek** connects South Amelia River and Nassau River. Its twisting channel leads through tidal flats and between oyster bars. **Sawpit Creek** enters the sound from the westward. Route A1A highway bridge, crossing the creek about 0.3 mile above the mouth, has a 38-foot fixed span with a clearance of 15 feet. A portion of this creek forms a part of the Intra-Coastal Waterway.

**Talbot Island**, about 5 miles in length and 1.5 miles in width, is partly wooded and partly marshy. Along the marshy eastern shore flow several creeks which separate Talbot and Little Talbot Islands. Talbot Island, Little Talbot Island, and Fort George Island form a State park and recreation area and are connected to Amelia Island and the mainland by a paved highway and bridges. The road also leads to Jacksonville along the north bank of the St. Johns River with a ferry connection at Fort George Island to the south bank of Mayport.

**Little Talbot Island**, a strip of low flat land about 4 miles long and averaging about 0.8 mile wide, lies in a north-south direction. The island is wooded along its outer coast. From seaward it shows a strip of dark woods with many conspicuous sand dunes near the beach. Its south end runs off in a low point of bare sand bordering on Fort George Inlet.

**Fort George Inlet** is a narrow body of water separating Little Talbot and Fort George Islands. The inlet changes rapidly due to shifting sands at its entrance. The **Heckscher Drive (State Routes 105-A1A) Highway Toll Bridge (Fig 1614.4)** near the entrance to the inlet has 38-foot fixed span with a clearance of 15 feet at the center. An overhead power cable at the bridge has a clearance of 40 feet. A fish camp is on the west bank

[Reserved photo bridge Fig 1614.4]

a

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-35
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

immediately above the bridge.

**Fort George Island** is westward and southward of Fort George Inlet. Its eastern shore, forming the coastline, shows a broad strip of white sand beach backed by a range of high hills. The island is separated from the mainland by Sisters Creek.

The coast from St. Johns River to Cape Canaveral trends south-southeastward for 125 miles. Three inlets, St. Augustine, Matanzas, and Ponce de Leon indent the coast. From St. Johns River to Ponce de Leon Inlet the coast is a continuous range of sand dunes backed by woods. The section southward of Ponce de Leon Inlet for 25 miles is formed by a very narrow strip of lowland lying between the sea, Indian River North, and Mosquito Lagoon. From seaward this coast shows a low line of sand dunes partially covered by grass and scrub trees with distant woods showing over them. The only natural object distinctive in appearance is Turtle Mound, a green hillock about 10 miles south of Ponce de Leon Inlet. The woods in the vicinity of Cape Canaveral are farther back from the beach and are less distinct when seen from seaward.

The depths from St. Johns River to Cape Canaveral are irregular. Depths of 5 to 7 fathoms are 1 mile offshore, while a depth of 3 fathoms is within 0.4 mile of the shore except off the entrances to St. Johns River, St. Augustine Inlet, Ponce de Leon Inlet, and from about 7 miles north of False Cape to Cape Canaveral. A 179°-359° measured nautical mile is just southward of the entrance to St. Johns River; the markers are located northward and southward of St. Johns Light. A submerged instrument platform that extends about 6 feet from the bottom is 5.8 miles south of St. Johns river in about 30°18.1'N., 81°23.0'W. Shoal spots with depths of 33 to 38 feet are from 4 to 6 miles offshore and from 12 to 16 miles north-northeastward of St. Augustine Light. These shoals are about 8 miles long in a southeasterly direction and about 2.5 miles wide. A swash channel with depths of 40 to 50 feet is inside these shoals.

Off Ponce de Leon Inlet 10 fathoms will be found within 2 miles of the beach. A wreck with 35 feet over it and shoals with a least depth of 35 feet are 5 to 7 miles north-northeastward of Ponce de Leon Inlet, and privately marked and unmarked fish havens extend 11 miles offshore northeastward and 13 miles offshore southeastward of the inlet. A dangerous sunken wreck is about 1.7 miles east-southeast of the inlet. Going southward the 10-fathom curve gradually works offshore to a distance of 10 miles off False Cape. From about 7 miles north of False Cape to Cape Canaveral there are dangerous shoals.

**St. Augustine and Vicinity:** St. Augustine Inlet is 30 miles south of the St. Johns River entrance. St. Augustine, the oldest city in the United States is 2 miles inside the entrance. Fort San Marco is a prominent historic landmark found there. The coast between St. Johns River and St. Augustine Inlet is straight with the 5-fathom curve about 0.5 mile offshore except at the entrances.



Figure 1614.5

**St. Augustine Channels and Anchorages (Fig 1614.5):**

The entrance channel to St. Augustine Inlet is subject to frequent change in depth and direction due to current and storm action; it is protected by a partial groin on the north side and by a jetty on the south side. Dangerous and shifting shoals extend 1 mile seaward. A lighted whistle buoy marks the approach, and buoys mark the channel. These aids are not charted since they are moved frequently with changing conditions to mark the best water. There is good anchorage in the Matanzas River at St. Augustine both below and above the Bridge of Lions. This anchorage, however, is not used as a harbor refuge because during strong northeasterly and northwesterly

winds the sea makes the bar impassable even for small vessels. A more protected anchorage in depths of 20 feet, hard sand bottom, is reported in Salt Run, close south-southeastward of St. Augustine Inlet.

The Intra-Coastal Waterway enters the St. Augustine Inlet from the north through Tolomato River and continues southward through Matanzas River. The San Sebastian River flows past the west side of the city

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-36
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

of St. Augustine and empties into the Matanzas River 1.4 miles south of the Route A1A highway bridge. In 1996, the controlling depth in the channel, marked by daybeacons, was 6 feet (8 feet at midchannel) to Kings Street Bridge. The overhead power cable crossing the river about 300 yards south of the Kings Street Bridge has a clearance of 66 feet.

**St. Augustine Harbor regulations and Facilities:** A dockmaster controls moorage at the city yacht pier. A number of small private landings are on the east side of the city, north and south of the bridge. The city yacht pier is about 100 yards south of the Bridge of Lions which crosses the Matanzas River opposite the center of the city. In 2002, an alongside depth of 18 feet was reported.

A privately marked channel with a reported controlling depth of 5½ feet in 2002 leads to a marina on the west side of Salt Run.

An extensive shrimp industry is conducted along the wharves in the upper part of the river, being supplied by seagoing shrimp boats during the shrimp season. Several small shipyards and shrimp boatbuilding yards are along the river. Shrimp boats up to 150 feet long can be handled for general repairs.



Figure 1614.6

**Matanzas Inlet and vicinity (Fig 1614.6):** Matanzas Inlet is 11 miles southward of St. Augustine Light. It affords an outlet for Matanzas River, which extends northward to St. Augustine and southward, following the coast for a distance of 8 or 10 miles to Graham Swamp. The inlet is obstructed by a shifting bar, and breakers extend across the entire entrance in normal weather. However, in May 1983, it was reported that with local knowledge about 3 feet could be carried through the entrance. The Intra-coastal Waterway passes through a land cut of the Matanzas River just inside the entrance.

State Route A1A highway bridge across the inlet has a 41-foot fixed span with a clearance of 10 feet. An overhead power cable crossing on the west side of the bridge has a clearance of 32 feet. Fort Matanzas National Monument is about 1 mile northwestward of the inlet.

Marineland, 13.6 miles southward of St. Augustine Light, is a conspicuous building housing an oceanarium. Flagler Beach is 26.5 miles southward of St. Augustine Light. The microwave tower and ocean pier are good landmarks. The T-shaped pier extending offshore is 650 feet long and 20 feet wide. Daytona Beach is a popular winter resort about 42 miles southward of St. Augustine Light. The buildings, water tanks, and radio towers are visible from seaward. The large recreation pier on the oceanfront is a prominent landmark for passing vessels.

The San Sebastian River joins the Intracoastal Waterway one mile south of downtown St. Augustine. It is the home of several marinas and the production facility for Mainship and Luhrs Yachts.

**Ponce De Leon Inlet and vicinity (Fig 1614.7):**

Ponce de Leon Inlet (see chart 11485) is 53 miles southward of St. Augustine Light and 41 miles northwestward of Cape Canaveral Light. It is used by both recreational and small commercial vessels bound for New Smyrna Beach or Daytona Beach, as well as others entering for an anchorage. Ponce de Leon Inlet Light (29°04'50"N, 80°55'41"W), 159 feet above the water, is shown from a red brick conical tower on the north side of the inlet. The inlet, protected at the



Figure 1614.7

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-37
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

entrance by jetties, is entered through a channel that leads over a bar and through the jetties. The outer end of the north jetty is marked by a light, and the inner end of the jetty is awash. In June 2002, severe shoaling existed across the entire channel. To prevent silting, a weir is at the inshore end of the north jetty and an impoundment basin is close southward. The current through the inlet is strong. It is reported that the average ebb is 3 knots, however, this can increase to 5 or 6 knots with southeasterly winds. The mean range of tide is 2.3 feet, and high water occurs about the same time as at Mayport.

Inside the inlet, three channels lead to the Intra-Coastal Waterway; northward through Halifax River, westward through Rockhouse Creek, and southeastward through Indian River North. The channels through Halifax River and Indian River North are marked by buoys. In May 2001, the controlling depth was 1.0 foot in the left outside quarter of Halifax River; thence in 1986, the midchannel controlling depth in Rockhouse Creek was 7 feet; thence in May 2001, using local knowledge, 1.1 feet could be carried to the Intra-Coastal Waterway by way of Indian River North.

About 10 miles southward of Ponce de Leon Inlet is Turtle Mound, a prominent hill 50 feet high. It is under the protection of the Florida State Historical Society. The original Indian name was Mount of Surruque. It was charted on Florida maps in 1564. Spanish galleons stopped here for repairs, wood, and water. Eldora is a fishing camp 11.5 miles southward of Ponce de Leon Inlet. False Cape, about 7.5 miles northward of Cape Canaveral Light, is the name given to a small part of the coast which it resembles when seen from seaward.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-38
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



## 1615 Port Canaveral – Chart 11478 – Port ID# 12716 – UN Locator Code USPCA

**Port Canaveral and Vicinity:** The John F. Kennedy Space Center and the Cape Canaveral Air Force Station occupy most of Canaveral Peninsula and Merritt Island, the large land areas between the ocean and the Banana and Indian Rivers, from Mosquito Lagoon on the north to Port Canaveral on the south. The huge Vehicle Assembly Building at the center, said to be one of the world's largest buildings, is visible far from shore. When closer in, other buildings and the mobile service towers at the cape are also conspicuous from all directions.

See Diagram 1615.1 for population density information

Trawlers or other vessels should exercise caution while dragging the ocean floor within a 25-mile radius of Cape Canaveral because missile debris containing unexploded ordnance exists in the area. Ordnance disposal personnel occasionally detonate explosives on the beaches in the vicinity of the cape.

Cape Canaveral, where the coast makes a sharp bend westward, is low and sandy. The shore in the vicinity of the cape is constantly moving eastward. Cape Canaveral Light (28°27'37"N, 80°32'36"W), 137 feet above the water, is shown from a white and black horizontally banded conical tower 1 mile inshore from the cape.

A Security Zone has been established to include certain land and water areas at Port Canaveral and adjacent areas at Kennedy Space Center and Cape Canaveral Air Force Station. During certain operations the Security Zone may be temporarily expanded. See 33CFR165.755.

Shoals extend 13 miles north and northeast from Cape Canaveral; mariners should use care when in the vicinity of the shoals. The outer shoals consisting of Hetzel Shoal, Ohio Shoal, and The Bull have a least depth of 11 feet. The inner shoals consisting of Chester Shoal and Southeast Shoal have depths of 2 to 18 feet. A lighted whistle buoy is 2.5 miles northeast of Hetzel Shoal. A lighted buoy is off the southeast end and along the south side of Southeast Shoal. In a heavy sea the shoals are marked by breakers, but with a smooth sea there is nothing to indicate them except their relative positions to Cape Canaveral Light and the lighted buoys. Only small light-draft vessels in calm seas should pass inside the outer shoals. Several wrecks are east of Cape Canaveral within 13 miles of the shore. They have been cleared by a wire drag to a least depth of 43 feet. An unmarked sunken wreck is north of Ohio Shoal in about 28°39.7'N., 80°23.3'W.

A danger zone for missile testing extends 3 miles offshore from False Cape to the entrance to Port Canaveral. See 33CFR165.755. Canaveral Bight, on the south side of the cape, is in the danger zone.

Port Canaveral is 4 miles southwest of Cape Canaveral Light and 150 miles south of the entrance to the St. Johns River. The city of Cape Canaveral is just southward of the port. The principal commodities handled in the harbor are petroleum products, cement, asphalt, salt, general cargo, citrus products, and newsprint. Commercial party fishing vessels, cruise ships, and many pleasure crafts operate from the port.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-39
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**Channels (Fig 1615.1):** A U.S. Navy project for Port Canaveral provides for an entrance channel 44 feet deep to East Basin, thence 41 feet in East Basin. A Federal project provides for a channel 40 feet deep from East Basin to Middle Basin, thence 35 feet deep in Middle Basin, thence 31 feet deep from Middle Basin to West Basin, and thence 31 feet in West Basin. The harbor is maintained at or near project depths. The entrance to the harbor is protected by jetties. The approach channel is marked by white 310° lighted range and lighted buoys; the entrance channel between the jetties is marked by a green 270° lighted range, a light, and lighted and unlighted buoys. The entrance to East Basin is marked by a red 325°30' lighted range. **Canaveral Barge Canal (Fig 1615.2)** leads westward to Banana River and the Intracoastal Waterway from the western end of the harbor just west of West Basin entrance. The Navy pier on the east side of Middle Basin is within a restricted area, and East Basin is within a danger zone. See 33CFR165.754.



Figure 1615.1

From southward of the shoals at Cape Canaveral to Bethel Shoal, a distance of about 43 miles, the shore is straight. The 5-fathom curve is from 0.3 to 1 mile offshore along this section of the coast.

**Weather, Port Canaveral and vicinity:** Tropical cyclones are a threat from about June through November. There are roughly four peak periods within this season. A slight maximum occurs in early June while more defined peaks occur in early August, early September and mid-October. The probability of at least one occurrence of gales from a tropical cyclone in 1 year is about 36 percent while the chance of two occurrences drops to 6 percent.

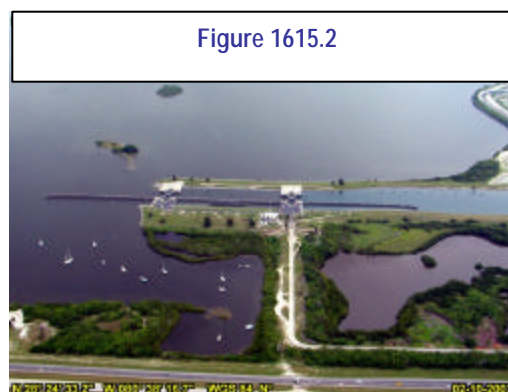


Figure 1615.2

Windspeeds of 17 knots or more are most likely from October through April when they occur 3 to 7 percent of the time at Cape Canaveral and 10 to 17 percent of the time at Patrick Air Force Base, about 13 miles south of the port. Thunderstorms are observed on about 70 days annually with a peak of 10 to 15 days per month from June through September. These are most likely during the late afternoon and early evening. Visibility is generally good, outside of showers. However, in December, January, and February, visibility drops below 0.5 mile (0.9 km) on about 2 to 4 days per month; they usually improve by midmorning. Temperatures only reach 90°F (32.2°C) or more on about 16 to 18 days annually but climb into the 80's (27.2° to 32.2°C) range on a little less than 200 days each year. Freezing temperatures are recorded just once or twice per year, on the average.

**Harbor regulations:** The Canaveral Port Authority has jurisdiction and control over port areas and facilities not under the control of the federal government. Vessels are ranked for movement priority. Emergency movements are first priority. Naval vessels engaged in demonstration and shakedown operations and regularly calling cruise ships have second priority. Generally all other vessels move on a first come, first served basis. Port regulations are contained in the Port Authority tariff. In addition, Operational Guidelines for the port have been promulgated by the Port Authority in consultation with the U.S. Coast Guard, U.S. Navy, U.S. Army Corps of Engineers, other interested parties and the pilots. Copies of both publications are available from Canaveral Port Authority, P.O. Box 267, Cape Canaveral, Florida 32920-0267. The Port Authority enforces regulations and assigns berths.

**Wharves:** Port Canaveral has commercial berths owned by the Port Authority. Middle and West Basins

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-40
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

are used by commercial vessels as well as at the north and south sides of the Inner Reach; cruise ships usually berth in the West Basin. Canaveral Port Authority maintains an internet website at [www.portcanaveral.org](http://www.portcanaveral.org). This internet site provides descriptions of port facilities and maximum allowable drafts. Information about facilities is also published in the U.S. Army Corps of Engineers Port Series No. 16.

#### Facilities on the south side of Inner Reach:

**Canaveral Port Authority, Cruise Terminals No. 4** (28°24'33"N, 80°35'46"W): 750-foot face; 31.5 to 33 feet alongside; deck height, 10.5 feet; mooring cruise vessels; boarding passengers; owned and operated by Canaveral Port Authority. (Cruise Terminals 2, 3 and 4 form a continuous berth, 2,153 feet long.) See USACE Port Series No. 16, Port ID 128.

**Canaveral Port Authority, Cruise Terminals Nos. 2 and 3 Wharf (Fig 1615.3)** (28°24'33"N, 80°36'00"W): 1,403-foot face; 31.5 to 33 feet alongside; deck height, 10.5 feet; mooring cruise vessels; boarding passengers; owned and operated by Canaveral Port Authority. See USACE Port Series No. 16, Port ID 129.



Figure 1615.3

**Canaveral Port Authority, South Cargo Piers 1, 2, and 3 (Fig 1615.4)** (28°24'36"N, 80°36'20"W): 1,615-foot face; 34 feet alongside; deck height, 10 feet; 108,000 square feet covered storage; 26 acres open storage; 2.5 million cubic feet cold storage; pipelines extend to storage tanks, 257,000-barrel capacity; roll-on/roll-off ramp at the east end of Pier 1; receipt and shipment of general cargo; receipt and shipment of petroleum products at Pier 3; receipt of paper products, asphalt; shipment of perishable food commodities; bunkering vessels; mooring pilot boats; owned by Canaveral Port Authority and operated by Canaveral Port Authority; Coastal Fuels Marketing, Inc.; and Mid-Florida Warehouses, Ltd. See USACE Port Series No. 16, Port ID 130.



Figure 1615.4

**Canaveral Port Authority, Tanker Berth No. 1** (28°24'34"N, 80°36'32"W): 45-foot face; 340 feet of berthing space with dolphins; 36 to 38 feet alongside; deck height, 10 feet; storage silo for 32,000 tons of cement; pipelines extend from wharf to storage tanks, 257,000-barrel capacity; receipt of petroleum products; asphalt, and cement; bunkering vessels; owned by Canaveral Port Authority and operated by Coastal Fuels Marketing, Inc.; Transtate Industrial Pipeline Systems, Inc.; and Continental Cement of Florida, Inc. See USACE Port Series No. 16, Port ID 131.

**Canaveral Port Authority, Tanker Berth No. 2** (28°24'34"N, 80°36'37"W): 65-foot face; 340 feet of berthing space with dolphins; 38 feet alongside; deck height, 10 feet; pipelines extend from

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-41
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

wharf to storage tanks, 250,000-barrel capacity; receipt and shipment of No. 6 fuel oil; owned by Canaveral Port Authority and operated by Transtate Industrial Pipeline Systems, Inc., and Exceltech Corp. See USACE Port Series No. 16, Port ID 132.

**Canaveral Port Authority, South Cargo Pier 4** (28°24'32"N, 80°36'40"W): 400-foot face; 400 feet of berthing space; 38 feet alongside; deck height, 10 feet; open storage area at rear for about 25,000 tons of salt; receipt and shipment of general cargo; receipt of salt and paper products; shipment of perishable food commodities; owned by Canaveral Port Authority and operated by Canaveral Port Authority; Mid-Florida Freezer Warehouses, Ltd., and Cargill, Inc., Salt Division. (Tanker Berths 1 and 2, and South Cargo Piers 4 and 5 form a continuous berth, 1,247 feet long.) See USACE Port Series No. 16, Port ID 133.

**Facilities on the north side of Inner Reach:**

**Canaveral Port Authority, North Cargo Piers 1 and 2 (Fig 1615.5)** (28°24'45"N, 80°36'43"W): 1,260-foot face; 1,350 feet of berthing space with dolphins; 38 feet alongside; deck height, 10 feet; crawler cranes to 165 tons; roll-on/roll-off ramp at north end; receipt of containerized and roll-on/roll-off general cargo; receipt of salt; owned by Canaveral Port Authority and operated by Canaveral Port Authority; Morton International, Inc., and Mid-Florida Freezer Warehouses, Ltd. See USACE Port Series No. 16, Port ID 155.



Figure 1615.5

**Canaveral Port Authority, North Cargo Pier 3** (28°24'39"N, 80°36'47"W): 400-foot face; 400 feet of berthing space; 32 feet alongside; deck height, 10 feet; 600,000 square feet covered storage; receipt and shipment of general cargo; mooring vessels; owned and operated by Canaveral Port Authority. See USACE Port Series No. 16, Port ID 154.



Figure 1615.6

**CSR Rinker Materials Corp., Port Canaveral, North Cargo Pier 4 (Fig 1615.6)** (28°24'39"N, 80°36'56"W): 400-foot face; 400 feet of berthing space; 34 feet alongside; deck height, 10 feet; one traveling gantry ship unloader, receipt of cement; mooring vessels; owned by Canaveral Port Authority and operated by CSR Rinker Materials Corp. See USACE Port Series No. 16, Port ID 153.



**Canaveral Port Authority, Cruise Terminal 5 (Fig 1615.7)** (northwest corner of West Basin): 565 feet of berthing space; 35 feet alongside; 59,000 square feet embarkation and baggage facility; mooring cruise vessels; boarding passengers; owned and operated by Port Canaveral Authority. See USACE Port Series No. 16, Port ID 147.



Figure 1615.7

**Canaveral Port Authority, Cruise Terminal 8** (south of Cruise Terminal 5): 800 feet of berthing space; 35 feet alongside; 70,000 square feet embarkation and baggage facility; mooring cruise vessels; boarding passengers; owned and operated by Port Canaveral Authority. See USACE Port Series No. 16, Port ID 146.

**Canaveral Port Authority, Cruise Terminal 9&10** (south of Cruise Terminal 8): 724 feet of berthing space; 33.5 feet alongside; 75,000 square feet embarkation and baggage facility; mooring cruise vessels; boarding passengers; owned and operated by Port Canaveral Authority. See USACE Port Series No. 16, Port ID 145.

## 1620 Economic Characteristics

This section outlines the maritime economic characteristics for the Northeast and Eastern Central Florida. This section is organized as follows:

- 1621 Fernandina, Florida and Kings Bay, Georgia
- 1622 Jacksonville, Florida
- 1623 Port Canaveral, Florida

### 1621 Fernandina, Florida, and Kings Bay, Georgia

Kings Bay is the home of U.S. Navy Submarine Group 10. Fernandina receives commercial containerized and break-bulk cargo. All bulk oil services are provided via the Intra-Coastal Waterway and are predominately heavy fuel oil for energy/pulp facilities. A limited number of inspected small passenger vessels operate from Fernandina for tourism and fishing. Fernandina is home to a significant commercial fishing vessel fleet.

The Port of Fernandina is Florida's northern-most natural deep water seaport serving the Southeastern United States and Gulf States. Major metropolitan areas served include Tampa, Orlando, Jacksonville, Atlanta, New Orleans and Houston.

The Port of Fernandina is a general cargo terminal, specializing in forest products, and a container terminal facility. The terminal is served by the CSX Rail Road including double stack container trains and all major regional and national truck companies. The Port of Fernandina is located very near the Interstate Highway System, only 14 miles from I-95 connecting to the east/west I-10 corridor.

The Port of Fernandina is located on Amelia Island within the City of Fernandina Beach. Two paper mills, Smurfit-Stone and Rayonier are adjacent to the port. In addition, twelve other paper mills as far north as Tennessee and Virginia serve the Port of Fernandina. The major commodities include Kraft Liner Board, Wood Pulp and Lumber. In addition to breakbulk, the Port of Fernandina caters to the independent container liner services predominately serving the north/south trade lanes and the Caribbean. Major commodities include refrigerated and chilled cargos, auto parts, consumer goods and machinery.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-43
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

With an eleven acre container terminal and 200,000 square feet of on port of warehouse space the port handles over 360,000 tons of breakbulk cargo and 24,000 TEUs of containers. Major trading partners include Venezuela, Colombia, Ecuador, Jamaica, Haiti, Dominican Republic, Brazil, Chile, Bermuda, Northern Europe and the Mediterranean. Domestically, Puerto Rico is a major trading partner.

### **Fernandina Freight Traffic**

According to the U.S. Army Corps of Engineers Jacksonville District, Fernandina moved over 615,000 short tons of freight (all commodities) during 2002, the most recent year for which data has been compiled, verified, and analyzed. Of this tonnage, approximately 143,000 tons were inbound on foreign vessels, 327,000 tons were outbound on foreign vessels, and 145,000 tons were shipped on domestic vessels. Of the domestic tonnage, only 37,000 tons was domestic coastwise trade, while the remaining 108,000 tons were internal receipt freight. According to U.S. Army Corps of Engineers footnotes, 526 tons of foreign inbound freight transitted through Fernandina for offloading in subsequent ports of call, and almost 33,000 tons of foreign outbound freight transitted through Fernandina having been loaded in previous ports of call but destined for foreign port delivery.

Freight tonnages in Fernandina are relatively stable since 1993, remaining in the range of between 550,000 short tons per year (total traffic) and 650,000 short tons per year. Freight totals peaked in 1999 at 644,000 short tons, and have declined to the 2002 total of 615,000 short tons.

Of the freight shipped through Fernandina, 49 tons were petroleum products, 114 tons were bulk/crude materials (primarily forest products and pulp), 245 tons were primary manufactured goods (primarily paper and paperboard), 64 tons were food and farm products (primarily fruits and frozen foods), and 58 tons were manufactured equipment (primarily vehicles and parts). Approximately 19 tons of material shipped through Fernandina was not categorized by the U.S. Army Corps of Engineers.

### **Fernandina Vessel Traffic**

According to the U.S. Army Corps of Engineers Jacksonville District, Fernandina received over 1,172 vessel trips (foreign and domestic) for vessels over 18 feet in draft; 585 of these were inbound vessel trips, 587 were outbound trips. In general Fernandina received 280 foreign vessel trips (in and out), 305 U.S. vessel trips (in and out). Of the self-propelled vessel trips, 332 were passenger and dry cargo vessel trips (in and out), none were tankers, and 150 were tugs and tows. Of the non-self-propelled vessel trips, 16 (in and out) were dry cargo, and 87 were petroleum tank barges.

## **1622 Jacksonville, Florida**

The port of Jacksonville contains Naval Station Mayport (NAVSTA), home of Navy Surface Group Two and other carrier groups, Marine Corps Blount Island Command, Naval Fuel Depot Jacksonville, and Naval Air Station Jacksonville (NAS). Several key bridges cross the St. Johns River in or near Jacksonville along strategic highway and railway routes. Approximately seven miles from the Mayport jetties lies Blount Island, the primary commercial port. A secondary commercial port (Talleyrand Terminal) lies approximately fourteen miles from the jetties near the population center. Together these port terminals account for over 7 million tons of cargo including 708,000 TEUs, over 500,000 automobiles, and delivered in over 1,500 deep draft vessel arrivals. Jacksonville is also the principal U.S. embarkation port for large barge-line service to the Caribbean, principally Puerto Rico. Commercial oil terminals and bulk reception facilities lye between these two terminals. Jacksonville is home to over 100 inspected small passenger vessels and a significant commercial fishing fleet, including a portion of the fleet based in the port of St. Augustine.

### **Jacksonville Freight Traffic**

According to the U.S. Army Corps of Engineers Jacksonville District, jacksonville moved over 17,906,000

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-44
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

short tons of freight (all commodities) during 2002, the most recent year for which data has been compiled, verified, and analyzed. Of this tonnage, approximately 9,677,000 tons were aboard on foreign vessels, and 8,229,000 tons were shipped on domestic vessels. According to U.S. Army Corps of Engineers footnotes, 59,599 tons of foreign inbound freight transitted through Jacksonville for offloading in subsequent ports of call, and 28,562 tons of foreign outbound freight transitted through Jacksonville having been loaded in previous ports of call but destined for foreign port delivery.

Freight tonnages in Jacksonville have fluctuated since 1993, ranging from a 1995 low of 15,693,000 tons and peaking in 1998 at 21,190,000 tons. Freight totals dropped from a steady 19,000,000 per year before 2001 to a steady 17,500,000 after 2001.

Of the freight shipped through Fernandina, 1,293,000 tons of coal arrived on foreign vessels, with just 294,000 tons being shipped on domestic vessels. 2,962,000 tons of petroleum products arrived on foreign vessels, with 5,018,000 tons being shipped on domestic vessels, including coastwise receipts. Approximately 500,000 tons of chemicals of all varieties were shipped on foreign and domestic vessels, but almost 3,000,000 tons of bulk/crude materials (primarily soil, gravel, sand, rock, and stone) arrived on foreign vessels, with only 37,000 of these tons being shipped coastwise on domestic vessels. Jacksonville handled 573,000 tons of primary manufactured goods (mostly steel wire) on foreign vessels, and 218 tons aboard domestic vessels (primarily coastwise cement and lime receipts). During 2002, Jacksonville handled approximately 564,000 tons of food and farm products on foreign vessels (primarily frozen foods) and shipped approximately 521,000 tons on domestic vessels (again mostly frozen foods). Almost 950,000 tons of manufactured equipment (primarily vehicles) shipped on foreign vessels, with another 1,723,000 shipping on domestic vessels (primarily uncategorized manufacturing products). Approximately 250 tons of material shipped through Jacksonville was not categorized by the U.S. Army Corps of Engineers.

### **Jacksonville Vessel Traffic**

According to the U.S. Army Corps of Engineers Jacksonville District, Jacksonville received over 25,500 vessel trips (foreign and domestic) for vessels over 18 feet in draft; 12,777 of these were inbound vessel trips, 12,777 were outbound trips. In general Jacksonville received 1,495 foreign vessel trips (in and out), 11,282 U.S. vessel trips (in and out). Of the self-propelled vessel trips, 1,221 were passenger and dry cargo vessel trips (in and out), 191 were tankers, and 1,348 were tugs and tows. Of the non-self-propelled vessel trips, 504 (in and out) were dry cargo, and 1,000 were petroleum tank barges.

## **1623 Port Canaveral, Florida**

Port Canaveral is the second busiest cruise port in the world, with six cruise terminals and two more on the drawing board. During fiscal year 2002, 3.8 million revenue cruise passengers passed through the Port's exquisite cruise terminals. During 2003, Norwegian Cruise Line will bring the *Dawn* to Port Canaveral. Carnival will replace the *Pride* with the new and larger *Glory*. Royal Caribbean will bring in the mammoth *Mariner of the Seas* to join *Sovereign of the Seas*. Also, 2-day cruises return with Ocean Club Cruises joining the Port's family of homeported ships. While the cruise industry continues to expand at Port Canaveral, the cargo business also is emerging as a major economic contributor to Central Florida. Last year, cargo had a total of 4.2 million short tons.

Foreign Trade Zone 136 at Port Canaveral, the world's first quadramodal zone, connects cargo by sea, land, air and space. It is among the largest general purpose zones in the country with 4,160 acres. It serves as a strong economic development tool, making local businesses more competitive in the international marketplace. Having the shortest direct entry on Florida's East Coast, Port Canaveral offers 45-minute transit time from the first sea buoy to docking.

Port Canaveral has two liquid bulk facilities and nine dry cargo berths with 6,976 feet of berthing space, including two Roll On/Roll Off (Ro/Ro) ramps available for its customers. Future plans call for the

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-45
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

construction of additional cargo berths in the north cargo area.

Port Canaveral's South Cargo Piers 1, 2, 3 4 and 5 provide more than 3,200 feet of docks for petroleum, frozen and perishable food shipments and other general cargo. Covered dry freight storage capacity on port property totals 750,000 square feet. The Port's cargo tonnage in Fiscal Year 2002 ended with an ending volume of 4.2 million tons. A multi-year plan is underway to grow cargo tonnage at Port Canaveral and to meet the market demands of the future. A direct result of this diversification effort will be the development of a dry bulk conveyor system from the south cargo piers to a private terminal adjacent to the Port.

### **Canaveral Freight Traffic**

According to the U.S. Army Corps of Engineers Jacksonville District, Port Canaveral moved over 3,981,000 short tons of freight (all commodities) during 2002, the most recent year for which data has been compiled, verified, and analyzed. Of this tonnage, approximately 2,284,000 tons were inbound on foreign vessels, 550,000 tons were outbound on foreign vessels, and 1,149,000 tons were shipped on domestic vessels. Of the domestic tonnage, only 472,000 tons were domestic coastwise trade, while the remaining 650,000 tons internal receipt and intra-port freight. According to U.S. Army Corps of Engineers footnotes, 249 tons of foreign inbound freight transitted through Canaveral for offloading in subsequent ports of call, and almost 423 tons of foreign outbound freight transitted through Canaveral having been loaded in previous ports of call but destined for foreign port delivery.

Freight tonnages in Port Canaveral are relatively stable since 1993, remaining in the range of between 3.5M short tons per year (total traffic) and 4.3M short tons per year. Freight totals peaked in 2001 at 4.3M short tons, and have declined to the 2002 total of 3,981,000 short tons.

Of the freight shipped through Canaveral, 2,116,000 tons were petroleum products, just one ton of chemicals was shipped, 487 tons were bulk/crude materials (primarily soil, sand, gravel, and rock), 1,098,000 tons were primary manufactured goods (primarily cement and concrete), 245,000 tons were food and farm products (primarily fruits and fruit juices), and 18,000 tons were manufactured equipment (various types). Approximately 16,000 tons of material shipped through Port Canaveral was not categorized by the U.S. Army Corps of Engineers.

### **Canaveral Vessel Traffic**

According to the U.S. Army Corps of Engineers Jacksonville District, Canaveral received over 3,000 vessel trips (foreign and domestic) for vessels over 18 feet in draft; 1,507 of these were inbound vessel trips, 1,539 were outbound trips. In general Canaveral received 850 foreign vessel trips (in and out), 680 U.S. vessel trips (in and out). Of the self-propelled vessel trips, 670 were passenger and dry cargo vessel trips (in and out), 45 were tankers, and 390 were tugs and tows. Of the non-self-propelled vessel trips, 54 (in and out) were dry cargo, and 8 petroleum tank barges.

## **1630 Area Charts and Maps**

- 1631 Northeast and Eastern Central Florida Area
- 1632 St. Marys River and Fernandina, chart 11503
- 1633 St. Johns River and Jacksonville, chart 11486
- 1634 Intracoastal Waterway and Coastline, chart 11488-11481
- 1635 Port Canaveral, chart 11478
- 1636 Population Density Maps
  - 1636.1 Nassau County Population Density (1990 Census)
  - 1636.2 Duval County Population Density (1990 Census)
  - 1636.3 St. Johns County Population Density (1990 Census)
  - 1636.4 Volusia County Population Density (1990 Census)
  - 1636.5 Brevard County Population Density (1990 Census)

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-46
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



1636.1 Nassau County Population Density

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-47
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

1636.2 Duval County Population Density

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-48
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1636.3 St. Johns County Population Density

VERSION DATE	V_1.1 26 May 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-49
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1636.4 Volusia County Population Density

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-50
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

1636.5 Brevard County Population Density

VERSION DATE	V_1.1 26 May 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-51
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1640 Information Characteristics

The three regional ports in Northeast and Eastern Central Florida, along with the secondary ports and the upper St. Johns River, Upper St. Marys River, and the Intra-coastal Waterway share identical port information characteristics. The federal government receives and tracks information about cargo, port shipments, vessel movements, and merchant/port personnel in real time through the Advance Notice of Arrival system and other raw data systems, synthesizes that information into a Common Tactical Picture, and shares that portrait of what “does and does not belong” with State and Local partners through both the Maritime Joint Task Force, the FBI’s Joint Terrorism Task Force, and the State of Florida’s Regional Domestic Security Task Force. The ports do not have a Vessel Traffic Service, Joint Harbor Operations Center, or other sensor network augmenting the Common Tactical Picture. Surveillance systems including cameras and other port sensors exist, but do not cover the entire harbor area.

## 1700 Links to Other Federal, State, and Local Governmental Security and Response Plans

This Area Maritime Security Plan is part of a comprehensive web of governmental security and response plans, and exists to supplement those plans to the extent that they do not fully address or draw together all elements necessary to guarantee the security of the maritime sector. Accordingly, this plan references other plans; the relationship to and contents of those plans are overviewed as follows:

- 1710 Federal Security and Response Plans
- 1720 Florida State and Local Security and Response Plans
- 1730 Georgia State and Local Security and Response Plans
- 1740 Vessel and Facility Security Plans

## 1710 Federal Security and Response Plans

This section considers security and emergency response plans intended to support the operations of those federal agencies that might be called upon at any time to lead a multi-agency response to a terrorist act, or threat of a terrorist act, in the United States. The Federal Maritime Security Coordinator recognizes that many plans may be used during an incident, particularly by the private and public sectors, at local and regional levels, and that other federal plans may be implemented to support the plans included in this analysis. These plans are:

- 1711 DRAFT National Response Plan (NRP)
- 1712 U.S. Government Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN)
- 1713 Federal Response Plan (FRP)
- 1714 Federal Radiological Emergency Response Plan (FRERP)
- 1715 National Oil and Hazardous Substances Pollution Contingency Plan (NCP)
- 1716 Department of Defense Plans

## 1711 National Response Plan (NRP)

[RESERVED]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-52
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



## 1712 U.S. Government Interagency Domestic Terrorism Concept of Operations Plan

### Lead for development: Federal Bureau of Investigation

The CONPLAN provides overall guidance to federal, state, and local agencies concerning how the federal government will respond to a potential or actual terrorist incident or threat that occurs in the United States, particularly one involving weapons of mass destruction (WMD). The CONPLAN outlines an organized and unified capability for a timely, coordinated response by federal agencies to a terrorist threat or act. The mission of the CONPLAN is to establish conceptual guidance for assessing and monitoring a developing threat; notifying appropriate federal, state, and local agencies of the nature of the threat; and deploying the requisite resources to assist the Lead Federal Agency (LFA) in facilitating interdepartmental coordination of crisis and consequence management activities.

The U.S. Government Interagency Domestic Terrorism Concept of Operations Plan was developed based on the following authorities:

**Presidential Decision Directive 39:** U.S. Policy on Counter-terrorism (PDD 39), issued June 1995, addresses the U.S. policy on counter-terrorism. In this PDD, the United States takes a stand on the deterrence, response, and defeat of all terrorist threats and activity. Terrorist attacks, whether they occur domestically or elsewhere, will be regarded as a potential threat to national security, as well as a criminal act. Such actions will result in retaliation with appropriate U.S. force. PDD 39 iterates that the United States will pursue all efforts to “deter and preempt, apprehend and prosecute, or assist other governments to prosecute individuals who perpetrate or plan to perpetrate such attacks.”

**Presidential Decision Directive 62:** Combating Terrorism (PDD-62), issued in 1998, strengthens the roles and responsibilities of the federal agencies in responding to and preventing terrorism. Some of the responsibilities include capturing and prosecuting terrorists; improving security of the airlines, waterways, and roads; and protecting the nation’s computer-based systems that play an integral role in the U.S. economy. In order to reach these objectives, PDD 62 created the Office of the National Coordinator for Security, Infrastructure Protection and Counter-terrorism.

The CONPLAN designates FBI and FEMA, after consultation with DOJ, as leads for incidents involving terrorism, but it is not clear what role the “Lead” will play in coordinating other federal agencies’ activities or in working with responders from the private sector and state and local governments. For example, while the CONPLAN designates FBI as the lead agency for crisis management, there is some confusion among federal support agencies as to whether FBI will coordinate all federal activities, or focus primarily on law enforcement matters and resolution of disagreements with or among other federal agencies. The working agreement under this Area Maritime Security Plan is that the FBI will coordinate federal maritime issues through the Federal Maritime Security Coordinate and under this AMS Plan.

## 1713 Federal Response Plan, April 1999

### Lead for development: Federal Emergency Management Agency

The FRP facilitates the delivery of all types of federal response assistance to states and territories of the United States to help them deal with the consequences of significant disasters. The plan outlines the planning assumptions, policies, concept of operations, organizational structures, and specific assignments of responsibility to the 27 signatory federal departments and agencies in providing response assistance to supplement the state, local, and territorial response efforts. The FRP consists of a Basic Plan, Emergency Support Function (ESF) Annexes, Recovery Function Annex, Support Annexes, Incident Annexes, Appendices and Figures. The 12 ESF Annexes provide guidelines for federal support for emergency needs. The annexes include the federal scope and policies, a description of the emergency situation and its implications, a concept of operations, the roles and responsibilities of lead and support agencies, and a glossary of applicable terms. The

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-53
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

Terrorism Incident Annex is the first in a series of anticipated incident annexes.

The **Federal Response Plan** was developed on the basis of Public Law 93-288, also known as *the Robert T. Stafford Disaster Relief Act (Stafford Act)*. The Stafford Act provides the authority for the federal government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property. Under the Stafford Act, the President is authorized to:

1. Establish a program of disaster preparedness that uses services of all appropriate agencies;
2. Make grants to states, upon their request, for the development of plans and programs for disaster preparedness and prevention; and
3. Ensure that all appropriate federal agencies are prepared to issue warnings of disasters to state and local officials.

## 1714 Federal Radiological Emergency Response Plan

### **Lead for development: Federal Emergency Management Agency**

The FRERP establishes an organized and integrated capability for timely, coordinated response by federal agencies to peacetime radiological emergencies. The FRERP provides the federal government's concept of operations based on specific authorities for responding to radiological emergencies, outlines federal policies and planning considerations on which the concept of operations of this plan and federal agency-specific response plans are based, and specifies authorities and responsibilities of each federal agency that may have a significant role in such emergencies. The plan contains two sections; the first includes background, considerations, and scope, and the second describes the concept of operations for response.

The Federal Radiological Emergency Response Plan was enacted based on the following two authorities:

**Nuclear Regulatory Commission Authorization**, Public Law 96-295, June 30, 1980, Section 304. This authorization requires the President to prepare and publish a "National Contingency Plan" (subsequently renamed the FRERP) to provide for expeditious, efficient, and coordinated action by appropriate federal agencies to protect the public health and safety in case of accidents at commercial nuclear power plants.

**Executive Order (E.O.) 12241**. This E.O. delegates to the Director of FEMA the responsibility for publishing the FRERP for accidents at nuclear power facilities and requires that it be published from time to time in the Federal Register. Executive Order 12241 has been amended by Executive Order 12657, FEMA Assistance in Emergency Preparedness Planning at Commercial Nuclear Power Plants.

The key issue concerning the relationship between this Area Maritime Security Plan, the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) and the Federal Radiological Emergency Response Plan (FRERP) is that all three plans apply simultaneously during radiological responses. Consequently, coordination during a radiological emergency is needed between the Federal departments and agencies that can potentially respond under these three plans. In general, the FRERP delegates control over terrorist radiological incidents to the Environmental Protection Agency as LFA. The EPA then considers the issue to be managed under the National Contingency Plan, and as agreed between the Coast Guard and EPA in a Memorandum of Agreement, the Coast Guard will serve as the Federal On-Scene Coordinator in the Coastal zone. Therefore radiological incidents will normally (initially) be considered the responsibility of the USCG FOSC who is also the Federal Maritime Security Coordinator. The FMSC may petition the EPA under the existing MOU to take control of any specific incident and serve as the FOSC; such option may be exercised depending upon the scope of the FOSC/FMSC's involvement in other security-related issues for the area outside the immediate site of the radiological response.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-54
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1715 National Oil and Hazardous Substances Pollution Contingency Plan

### *Lead for development: Environmental Protection Agency*

The NCP describes the framework for the federal government's response to both discharges of oil and releases of hazardous substances, pollutants, and contaminants in the United States and its territories. It also provides for overall coordination in the event of such spills among the hierarchy of responders and contingency plans. The NCP establishes the NRT to provide national-level support for On-Scene Coordinators; coordinates a national program of preparedness, planning, and response; and facilitates research to improve response activities. EPA chairs the NRT. The plan also establishes RRTs to coordinate preparedness, planning, and response at the regional level and at the local (area) level in the inland zone.

The National Oil and Hazardous Substances Pollution Contingency Plan was first developed and published in 1968 in response to a massive oil spill from the oil tanker Torrey Canyon. The NCP provides the organizational structure and procedures for preparing for and responding to discharges of oil and releases of hazardous substances, pollutants, and contaminants. The NCP is required by section 105 of the Comprehensive Emergency Response, Compensation, and Liability Act of 1980 (CERCLA), Public Law Number 96-510 (Title 42 USC Section 9601 et seq.), as amended by the Superfund Amendments and Reauthorization Act of 1986 (SARA), Public Law 99-499 (42 U.S.C. 9662 et seq.) and by section 311(d) of the Clean Water Act (CWA), as amended by the Oil Pollution Act of 1990, Public Law 101-380 (33 U.S.C. 2701 et seq.; 104 Stat. 484).

Three executive orders have implications for hazardous materials: Executive Order 12088, Federal Compliance with Pollution Control Standards, as amended by Executive Order 12580, Superfund Implementation, as amended by Executive Order 12777 (56 FR 54757, October 22, 1991), Implementation of Section 311 of the CWA, as amended. In the Executive Order 12088, the President delegated to the head of each Executive agency the responsible for ensuring that all necessary actions are taken for the prevention, control, and abatement of environmental pollution with respect to Federal facilities and activities under the control of the agency. In Executive Order 12580, the President delegated to various Federal officials the responsibilities for implementing the CERCLA as amended by SARA. In Executive Order 12777, the President delegated to EPA the responsibility for the amendment of the NCP. Amendments to the NCP are coordinated with members of the NRT prior to publication for notice and comment. The NCP is applicable to response actions taken pursuant to the authorities under CERCLA and section 311 of the CWA, as amended.

## 1716 Department of Defense Plans

Representatives from DOD participated in the development of this report. Plans and directives, such as the US NORTHCOM Campaign Plan 2525-01 (FOUO); DOD Directive 3025.1; and JCS CONPLAN 0300/0400 of DOD were also considered as candidates for the analysis but were determined, like plans from the Department of Health and Human Services (HHS) and others, to fall into the category of plans or directives that assist responders acting in support of the federal lead operating under one of the four plans being reconciled in this analysis, and thus were not included.

DOD would normally respond in a support role in any federal government response to a terrorist incident in the United States. Under certain scenarios, however, DOD elements could be called upon under their Homeland Defense Mission to take tactical lead in neutralizing a terrorist threat approaching or already within U.S. jurisdiction. It is also possible that these same DOD elements may need to interact with other federal agencies and local responders operating at the scene of an incident under the plans being reconciled in this report. Procedures need to be developed to ensure DOD and other response organizations have secure communication, positive coordination, and as appropriate, transfer of information to make effective tactical decisions.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-55
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 1720 Florida State and Local Security and Response Plans

The State of Florida and each county within the state maintain both a Comprehensive Emergency Management Plan (CEMP - used by the Emergency Management community at State and County Emergency Operations Centers) and a Health Department Emergency Operations Plan. These plans (at both the state and county level) are the counterparts of this Area Maritime Security Plan. Within the county and state CEMPs, annexes related to various contingencies contain procedures and processes relevant to both prevention and responses under this plan. Similarly, the County EOP outlines processes and procedures for dealing with health crises, whether naturally occurring outbreaks or bioterrorism. In addition to the mandatory contingency annexes, many counties have developed recommended annexes based on their county's perceived emergency management needs. Both required and optional/recommended elements of the CEMPs and EOPs are outlined below. Future versions of this plan will include direct links to the various Florida county CEMP annexes related to the AMSP, and a brief overview of those annexes sufficient to understand the link to the AMSP.

	State of Florida	County Emergency Management	County Health Department
<b>REQUIRED PLANS AND PROCEDURES</b>			
Comprehensive Emergency Management Plan (CEMP)	X	X	
Emergency Operations Plan (EOP)			X
Terrorism Plan/Annex	X	X	
Mitigation Plan			
Emergency Operations Center Standard Operating Guidelines (EOC/SOG)	X	X	
Hazardous Materials Response	X	X	
<b>RECOMMENDED PLANS AND PROCEDURES</b>			
Hurricane Evacuation & Re-entry Plan	X	X	
Special Needs Plan (developed jointly with EM and HD)		X	X
Host Sheltering	X	X	
Bioterrorism Response		X	X
Temporary Housing	X	X	
Impact Assessment		X	
Damage Assessment		X	
Resource Management		X	
Volunteers & Donations Management	X	X	
Mass Casualty Incident Management		X	
Continuity of Government	X	X	

## 1730 Georgia State and Local Security and Response Plans

[RESERVED]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-56
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

# 1740 Vessel and Facility Security Plans

[RESERVED]

VERSION DATE	V_1.1 26 May 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	1000-57
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 2000 AREA MARITIME SECURITY COMMITTEE

This section defines the Jacksonville Maritime Transportation Exchange (JMTX) Port Security Committee and the Port Canaveral Security Committee, in accordance with Title 33 Code of Federal Regulations Section 103.300(b). Together, these port security committees fulfill the requirements of that regulation regarding Area Maritime Security. This section is organized as follows:

- 2100 [Introduction](#)
- 2200 [Purpose and Objectives](#)
- 2300 [Charter](#)
  - 2310 [Organization](#)
  - 2320 [Rules Governing the Port Security Committees](#)
  - 2330 [Rules Governing the Working Subcommittees](#)
  - 2340 [Rules Governing the Executive Subcommittee](#)
  - 2350 [Handling and Protection of Information](#)
  - 2360 [Amending the Charter](#)
- 2400 [Relationship to Other Committees](#)

## 2100 Introduction

The Commandant of the Coast Guard has determined that Port Security Committees (AMS Committees) are an essential tool necessary for the development and execution of Area Maritime Security Plans and for achieving an enhanced level of security within the maritime domain. As such, the Coast Guard Captain of the Port (COTP), acting as the Federal Maritime Security Coordinator (FMSC), has established and convened two Port Security Committees to advise the Coast Guard on maritime security matters. Effective on publication of the maritime security final rule 33 CFR Subchapter H, these two Port Security Committees were chartered to assure they conformed to the procedures established by 33 CFR 103.300. As such, they serve together to meet the AMS Committee requirements.

The Port Security Committees are open to the public, and all meetings of the Port Security Committee constitute public access meetings. Meetings closed to the public are conducted solely by the Executive Subcommittee. Port Security Committee records other than those marked as Sensitive Security Information under Section 3500 will be treated as governmental records maintained by the FMSC and are therefore subject to the Freedom of Information Act and the Privacy Act.

The area covered by this plan is defined in federal regulations at Title 33 Code of Federal Regulations part 3.35-20. In general, the area of Northeast Florida (including the extreme southern border area of Georgia) and Eastern Central Florida for which Port Security Committees have been established are divided as follows:

**JMTX Port Security Committee** – Northeast Florida including those parts of Baker, Clay, Duval, Flagler, Nassau, Putnam, and St. Johns Counties in Florida and Camden and Charlton Counties in Georgia, which fall within the bounds described in 33 CFR part 3.35-20.

**Port Canaveral Security Committee** – Eastern Central Florida including those parts of Brevard, Lake, Volusia, Seminole, Orange, and Osceola Counties, Florida, which fall within the bounds described in 33 CFR part 3.35-20.

See [Appendix 9910](#) for the signed, approved Port Security Committee charter.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------



## 2200 Purpose and Objectives

Under the federal regulations, the Port Security Committee brings appropriately experienced representatives from a variety of sources in the area together to continually assess security risks to the port(s), determine appropriate risk mitigation strategies, as well as develop, revise, and implement the AMS Plan. The Port Security Committee also serves under the federal plan as a mechanism by which security threats and changes in MARSEC Levels are communicated to port stakeholders.

The objectives of the Port Security Committee include:

1. Assist in the development, review, and update of the AMS Plan aimed at maintaining acceptable risk levels during normal operations and during times of heightened threats. The AMS Plan outlines scalable security procedures to be taken by MTS stakeholders to ensure the continued safety and security of our nation's port areas and MTS.
2. Assist with a comprehensive AMS Assessment. These assessments must detail the threats, vulnerabilities, and consequences to an attack in the port. This requirement may be completed using the Risk Based Decision-Making methodologies developed by the Coast Guard.
3. Integrate and/or amend existing security assessments of maritime facilities using agreed criteria.
4. Develop and adopt preventative security measures for appropriate MARSEC Level 1 (sustainable baseline) and Levels 2 and 3 to address increased threat conditions (both general and specific). The measures will meet consolidated requirements of all agencies having jurisdiction.
5. Develop information sharing procedures for threat warnings, response, intelligence gathering, and threat assessment among public and private entities.
6. Solicit stakeholder recommendations for continuing improvements of AMS measures.
7. Promote effective security measures that maintain or enhance operational efficiencies and minimize impact to legitimate trade.
8. Advise, consult with, report to, the FMSC on matters relating to maritime security in Northeast and Eastern Central Florida.
9. Assist the FMSC with the communication of security information to the port and waterway stakeholders.

## 2300 Charter

This document charters the Jacksonville Maritime Transportation Exchange (JMTX) Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee, in accordance with Title 33 Code of Federal Regulations Section 103.300(b). Together, these port security committees fulfill the requirements of that regulation regarding Area Maritime Security Committees. See Appendix 9910 for the signed copy of the charter. The charter is organized as follows:

- 2310 [Organization](#)
- 2320 [Rules Governing the Port Security Committees](#)
- 2330 [Rules Governing the Working Subcommittees](#)
- 2340 [Rules Governing the Executive Subcommittee](#)
- 2350 [Handling and Protection of Information](#)
- 2360 [Amending the Charter](#)

## 2310 Organization

This section outlines the organization of the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

Regulations Section 103.305(a). This section is organized as follows:

- 2311 [JMTX Jacksonville/Fernandina Port Security Committee](#)
- 2312 [Port Canaveral Security Committee](#)
- 2313 [Standing Committees](#)
- 2314 [Ad-Hoc Committees](#)

## **2311 The JMTX Jacksonville/Fernandina Port Security Committee**

The Jacksonville Marine Transportation Exchange (JMTX) is Jacksonville's maritime trade organization created to work for the success of its membership and coordinate the safe, secure and environmentally responsible management of the marine transportation system within the port of Jacksonville. JMTX's goal is to work in partnership with the port stakeholders to make Jacksonville the port of choice.

Somewhat unique as a maritime association, JMTX has been established to provide a stable coordinating structure for port-wide planning, coordination and infrastructure recommendations. JMTX serves as an information clearinghouse for port critical information, provides a forum for stakeholder issues and serves as a stakeholder advocate to local, regional and national agencies.

JMTX is a growing organization with more than 55 member companies and agencies. JMTX is structured around seven critical committees including: Port Security, Harbor Safety, Information Sharing, Maritime Infrastructure, Agents and Operators, Community Outreach and Environmental Protection. Port stakeholder involvement in these committees is wide spread and has not been limited to JMTX members.

JMTX has been accepted by the U. S. Coast Guard as the coordinating organization for the port's official Port Security Committee, and the Harbor Safety Committee. Since 9/11, JMTX has played a major role in coordinating security issues including assessments, intelligence sharing and compliance with security requirements.

The JMTX Jacksonville/Fernandina Port Security Committee brings together the resources and experience of law enforcement, regulatory agencies and port stakeholders to develop strategies and procedures to support the goals of port security.

The committee is jointly chaired by the Coast Guard Captain of the Port along with an industry leader.

The FMSC will designate a member of his/her staff as the Executive Secretary of the Port Security Committees for both Jacksonville and Port Canaveral. The Executive Secretary will be responsible for the administrative duties of the committees, such as the designation of members, publishing meeting agendas, taking of meeting minutes, and maintaining current editions of the AMS plan, including digital versions. The Executive Secretary is also responsible for ensuring that all committee records are properly maintained and designated SSI as appropriate.

## **2312 The Port Canaveral Security Committee**

The Port Canaveral Security Committee is a standing body of industry leaders, Department of Defense representatives, Port Authority representatives, NASA representatives, port law enforcement agencies, and emergency response contractors and governmental agencies. For many years, this informal body

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-3
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

has worked with the Coast Guard Captain of the Port in Jacksonville and the Marine Safety Detachment in Port Canaveral to coordinate the safe, secure and environmentally responsible management of the marine transportation system in Port Canaveral and the surrounding area.

The Port Canaveral Security Committee has been accepted by the U. S. Coast Guard as the port's official Port Security Committee. Since 9/11, the Port Security Committee has played a major role in coordinating security issues including assessments, intelligence sharing and compliance with security requirements.

The Port Canaveral Security Committee brings together the resources and experience of law enforcement, regulatory agencies and port stakeholders to develop strategies and procedures to support the goals of port security.

The committee is jointly chaired by the Coast Guard Captain of the Port's representative along with an industry leader.

## 2313 Standing Subcommittees

The JMTX Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee standing subcommittees shall generally be established/disestablished on the direction of the Co-Chairs to address long term issues or goals of either PSC. Any PSC Member may volunteer to serve on any standing subcommittee (except the Executive Subcommittee, see section 2345 below). An appointed member of the Executive Subcommittee shall chair each subcommittee. Co-Chairs of the PSC cannot service as Subcommittee Chairpersons. Chairpersons are responsible for the general supervision and coordination of the subcommittee, including scheduling meetings and recording results. Standing Subcommittees include:

- The Executive Subcommittee
- Subcommittee One: Regulatory Compliance and Membership
- Subcommittee Two: Port Security Planning
- Subcommittee Three: Security Exercise Planning and Evaluation
- Subcommittee Four: Special Events Planning
- The Maritime Joint Task Force

## 2314 Ad-Hoc Subcommittees

The JMTX Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee Ad-Hoc Subcommittees shall be chartered by the Co-Chairs to address specific issues or functions that are expected to be short term. Ad Hoc Subcommittees shall not normally remain active for more than one year.

## 2320 Rules Governing the Port Security Committees

This section outlines the rules governing the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal Regulations Section 103. This section is organized as follows:

### 2321 [Purpose and Scope of the Committees](#)

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-4
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

- 2322 [Membership in the Committees](#)
- 2323 [Meetings of the Committees](#)
- 2324 [Geographic Area of Responsibility of the Committee](#)

## 2321 Purpose and Scope of the Committees

**JMTX Jacksonville/Fernandina Port Security Committee.** The JMTX Jacksonville/Fernandina Port Security Committee exists to accomplish the following three goals:

- 1) The Port Security Committee will assist agencies and organizations with meeting the statutory requirements from both state and federal Seaport Security measures.
- 2) The Port Security Committee will support and assist the Federal Maritime Security Coordinator (USCG Captain of the Port), state and local agencies, and maritime stakeholders with assessment, planning and exercising of port security issues.
- 3) The Port Security Committee will serve as a forum for the exchange of intelligence, experience and ideas relating to maritime security issues.

**Port Canaveral Security Committee.** The Port Canaveral Security Committee provides a forum for port stakeholders in and near Port Canaveral to evaluate maritime vulnerabilities to terrorism and criminal activities and works to assist in the formulation of protection strategies and plans. The Committee also provides a link between law enforcement agencies and port industry members to help coordinate planning and activities.

## 2322 Membership in the Committees

**JMTX Jacksonville/Fernandina Port Security Committee.** All persons, firms, associations, agencies, and corporations of good standing in the community are eligible for membership in the Jacksonville Maritime Transportation Exchange and are free to join the Port Security Committee.

**Port Canaveral Security Committee.** All persons, firms, associations and corporations of good standing in the community are eligible for membership in the Port Security Committee. Membership is open to any interested commercial entity, government agency, or other marine transportation system stakeholder operating on, or along, or having jurisdiction over Port Canaveral and surrounding navigable waterways.

## 2323 Meetings of the Committees

Each Port Security committee shall meet as needed and called by the Chair, and in any case not less than once during each calendar year and preferably once each quarter. Additionally, the committee will meet when requested by a majority of the AMS committee members. The Chair shall determine the time and venue of the meetings. The Chair shall make arrangements for these meetings, preferably with a revolving “host” from amongst the subcommittee members. Meetings shall be open to the public and shall not cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information. Records of these meetings may be made available to the public upon request. However, FMSC’s will ensure that all material designated as SSI will be protected from disclosure to the public.

## 2324 Geographic Area of Responsibility of the Committees

The area covered by this plan is defined in federal regulations at Title 33 Code of Federal Regulations

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-5
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

part 3.35-20. In general, the area of Northeast Florida (including the extreme southern border area of Georgia) and Eastern Central Florida for which Port Security Committees have been established are divided as follows:

- **JMTX Port Security Committee** – Northeast Florida including those parts of Baker, Clay, Duval, Flagler, Nassau, Putnam, and St. Johns Counties in Florida and Camden and Charlton Counties in Georgia, which fall within the bounds described in 33 CFR part 3.35-20.
- **Port Canaveral Security Committee** – Eastern Central Florida including those parts of Brevard, Lake, Volusia, Seminole, Orange, and Osceola Counties, Florida, which fall within the bounds described in 33 CFR part 3.35-20.

## 2330 Rules Governing the Working Subcommittees

This section outlines the rules governing working subcommittees of the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal Regulations Section 103. This section is organized as follows:

2331 [Purpose and Scope of the Subcommittees](#)

2332 [Membership in the Subcommittees](#)

2333 [Officers of the Subcommittee](#)

2334 [Meetings of the Subcommittees](#)

2335 [Procedural Rules](#)

## 2331 Purpose and Scope of the Working Subcommittees

The purpose of the Port Security Committee's Working Subcommittees is to form a small, balanced nucleus of port stakeholders that meet the goals and objectives of the Port Security Committee. Specific objectives of the working subcommittees are:

### Subcommittee One: Regulatory Compliance and Membership

- Provide a regular forum for discussion of information relative to state and federal legislation and rulemaking.
- Provide a unified response to state and federal legislators to effect common rules for implementation.
- Assist stakeholders in the implementation of federal and state regulations.
- Sponsor Maritime Domain Awareness infrastructure for the port.

### Subcommittee Two: Port Security Planning

- **Area Maritime Security Plan:** Develop and execute a whole-port security coordination plan (similar to the Area Contingency Plan for pollution response) for all commercial and private stakeholders, and federal, state, and local government agencies with responsibilities in the port or on the waterways of Jacksonville.
- **“One-Method” Consensus Risk Assessment Methodology:** Develop and deploy a consensus Risk (consequence \* vulnerability\*threat) assessment methodology to be used by all government and private entities in the port.
- **“One-Format” Consensus Vessel and Facility Security Plan Templates:** Develop and deploy consensus vessel and facility security plan templates/formats which are based on

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-6
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

the “one-method” risk assessments and which incorporate all government agency requirements.

- **Develop Expertise:** Provide a support system in form of training, review, and comment to private companies and government agencies as they begin using the “one-method” Risk Assessment Methodology and “one-format” vessel and facility security plan templates.

#### **Subcommittee Three: Security Exercise Planning and Evaluation**

- **Annual Port Security Drills.** Design and execute Area Maritime Security Drills in the port at least once per year to exercise and improve the Area Maritime Security Plan for the port.
- **Stakeholder Drills.** Assist port stakeholders with the design and execution of their security drills and exercises as required by federal, state, and local regulation.
- **Collect and Share Best Practices.** Capture and share the lessons learned during exercises and develop best practices to share with all port stakeholders.

#### **Subcommittee Four: Special Events Planning**

- Synthesize special event security plans in coordination with the Maritime Joint Task Force and Subcommittee Two.

#### **Maritime Joint Task Force (Government)**

- Provide an intelligence briefing at the quarterly PSC General Membership meeting. The briefings will be in accordance with applicable state and federal laws related to classified information.
- Provide a two-way communication mechanism to provide critical port security information among law enforcement agencies and port stakeholders.
- Assist security incident prevention and response agencies to coordinate and cooperate.
- Through a series of Memoranda of Agreement between federal, state, and local government agencies, establish a systematic, standing joint agency security activity/patrol/mission planning and de-conflicting (JMP/D) process. The systematic process must assure the agencies: (1) jointly plan and conduct overlapping operations; (2) fully leverage each other's independent operations for mutual benefit; and (3) avoid unintentionally infringing upon each other's operations or unintentionally imposing redundant burdens on our customers.

## **2332 Membership in the Subcommittees**

Members will be assigned to serve in Subcommittees on a volunteer basis. Any general member of the Port Security Committee is eligible for membership in any subcommittee, except the Maritime Joint Task Force, which is composed solely of government agency representatives. Members will not be appointed and membership in the subcommittee will be highly informal and based on the member's willingness to serve.

Subcommittee members will not be required to submit to a security background examination.

## **2333 Officers of the Subcommittees**

The Chair of the each Subcommittee for each Port Security Committee will be a designated member of the Executive Subcommittee only. No other subcommittee officers need be appointed in order to maintain the open and informal working environment.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-7
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------



## 2334 Meetings of the Subcommittees

Each Executive Subcommittee shall meet as needed and called by the chair, and any case not less than once during each calendar year and preferably once each quarter. The Chair shall determine the time and venue of the meetings. The Chair shall make arrangements for these meetings, preferably with a revolving “host” from amongst the subcommittee members. Meetings shall be open to the Port Security Committee and shall not cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information. The Executive Subcommittee Chair shall schedule meetings to cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information restricted to the appointed members and select expert invitees separately; rules governing those sessions are described in section 2340 below.

## 2335 Working Subcommittee Procedural Rules

**Rule 1. Subcommittee Policy.** It is the policy of the Subcommittees that Port Security Committee members shall have the opportunity to speak to any Subcommittee meeting agenda item before final action.

**Rule 2. Scheduling of Closed Session.** Bearing in mind section 2351 of this charter (below), special closed sessions shall be scheduled to the extent possible and appropriate prior to Port Security Committee membership meetings. Any closed session may be scheduled during or after a general Port Security Committee meeting.

**Rule 3. Meeting Adjourned to Date Certain.** When a Subcommittee meeting is adjourned, it must in all cases be adjourned to another scheduled meeting date. All unfinished items will be listed in their original order after roll call on the agenda of such scheduled meeting.

**Rule 4. Agenda Matters.** The principle procedure for holding Subcommittee meetings will be an agenda. All meetings shall have an agenda.

**Rule 5. Quorum.** Subcommittees shall have no quorum and shall meet with any number of members present.

**Rule 6. Minutes.** The Subcommittees shall not be required to prepare and distribute minutes of its meetings. The Chair shall take notes; these notes need not be verbatim but shall reflect the sense of the discussion and any recommendation made with respect to each subject considered in subcommittee. A report of the subcommittee shall be delivered to the Port Security Committee during its quarterly meetings and to the Federal Maritime Security Coordinator upon request.

**Rule 7. Conduct of Subcommittee Meetings.** The chair of the Subcommittee may conduct meetings with as much informality as is consistent with these charter procedural rules. The views of interested private citizens may be heard in certain subcommittee meetings, but in no case shall a subcommittee meeting be used as a substitute for the Port Security Committee meetings.

## 2340 Rules Governing the Executive Subcommittee

This section outlines the rules governing the executive subcommittee of the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-8
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

(PCSC) in accordance with Title 33 Code of Federal Regulations Section 103. This section is organized as follows:

- 2341 [Purpose and Scope of the Executive Subcommittee](#)
- 2342 [Membership in the Executive Subcommittee](#)
- 2343 [Nomination and Appointment Process](#)
- 2344 [Acceptance and Pledge](#)
- 2345 [Officers of the Subcommittee](#)
- 2346 [Meetings of the Subcommittee](#)
- 2347 [Procedural Rules](#)

## 2341 Purpose and Scope of the Executive Subcommittee

The purpose of the Port Security Committee's Executive Subcommittee is to form a small, balanced nucleus of port stakeholders that steer the work of the Port Security Committee and meet the requirements for an Area Maritime Security Committee (AMSC), consistent with Title 33 Code of Federal Regulations Section 103.310. Responsibilities of the Executive Steering Subcommittee are:

- To chair the working subcommittees;
- To identify critical port infrastructure and operations;
- To identify risks (threats, vulnerabilities, and consequences) in the maritime sector;
- To complete an Area Maritime Security Assessment in accordance with 33 CFR Part 103, subpart D;
- To determine mitigation strategies appropriate to these risks and implementation methods;
- To develop and describe the process for continually evaluation the overall port security by considering consequences and vulnerabilities, how they change over time, and what additional mitigation strategies can be applied;
- To provide advice to and assist the Federal Maritime Security Coordinator in developing the Area Maritime Security Plan in accordance with 33 CFR Part 103 Subpart E;
- To design and recommend to the Federal Maritime Security Coordinator measures to assure effective security of infrastructure, special events, vessels, passengers, cargo and cargo handling equipment at facilities within the port and not otherwise covered under federally approved Vessel or Facility Security Plans;
- To serve as the principle link for communicating the Area Maritime Security Plan once approved, including any requirements for entities operating in the port contained in the Plan;
- To serve as the principle link for communicating threats and changes in Maritime Security Condition (MARSEC) levels;
- To serve as the principle link for disseminating appropriate security information to the Port Stakeholders;
- To serve to assist entities operating in the port in understanding and complying with Federal, State, and Local security regulations and requirements;
- To coordinate governmental security incident command-and-response through one of the AMSC subcommittees;
- To audit and revise the Area Maritime Security Plan on a regular basis and following experiences offering lessons learned;
- To coordinate the conduct of an Area Maritime Security Exercise at least once each calendar year;
- To maintain records of Port Security Committee operations and decisions.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-9
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

## 2342 Membership in the Executive Subcommittee

In accordance with Title 33 Code of Federal Regulations Section 103.305 (Composition of an Area Maritime Security Committee), the Executive Subcommittee must have not less than seven and no more than 50 (total) members appointed by the Federal Maritime Security Coordinator, each having at least five years experience related to maritime or port security operations (including broad state or local counter-terrorism responsibilities). The Executive Subcommittee members serve as the core or steering group for the JMTX Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee. Members will be assigned to serve on the JMTX Jacksonville/Fernandina Port Security Committee or the Port Canaveral Security Committee, but not both, in their Appointment Letter from the Federal Maritime Security Coordinator. Appointments will typically be for a five year period; members may be reappointed where warranted and furthering the purposes of the Executive Subcommittee.

Prior to appointment, nominated members will be required to submit to appropriate security background examinations to verify the identity and suitability of the nominee.

To be considered for appointment, nominees must be members in good standing of one of the following:

- Federal Governmental Agencies with Authority, Jurisdiction, or Interest in Maritime Homeland Security in Northeast Florida;
- State Governmental Agencies or Political Officials with Authority, Jurisdiction, or Interest in Maritime Homeland Security in Northeast Florida;
- Local public safety, crisis management, and emergency response agencies in Northeast Florida;
- Law enforcement agencies in Northeast Florida;
- Security organizations in Northeast Florida;
- Maritime industry;
- Other port entities or individuals having special competence in maritime security; or
- Other port entities or individuals likely to be affected by security practices and policies.

## 2343 Nomination and Appointment Process

The Federal Maritime Security Coordinator will, at his sole discretion, solicit the Port Security Committees for nominations for appointment to the Executive Subcommittee. Nominations will typically be made in writing to the Port Security Committee Co-Chairs. Nominations must detail how the nominee meets the requirements of section 2342 of this charter, and must explicitly state the willingness of the individual both to serve and to submit to the required security background examinations. Nominations may be submitted by the nominee him or herself, or by other persons. When a nomination is for another person, it must explicitly state whether the individual is aware of the nomination and is willing to serve.

Once the announced period for submitting nominations to the Executive Subcommittee elapses, the Port Security Committee Co-Chairs will compile lists and background information on all nominees and consult with the Executive Subcommittee on these nominees. Based on a majority vote, the Executive Subcommittee will forward a list of nominees recommended for appointment to the Federal Maritime Security Coordinator for final evaluation. When the nominations are deemed insufficient for the purposes of the Executive Subcommittee, the Subcommittee may take action to recruit nominations from individuals who had not considered appointment, and may reconvene to consider these additional nominations. In no case shall this process extend more than 30 days after the close of the announced period.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-10
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

In consultation with the Port Security Committee Co-Chairs, the Federal Maritime Security Committee will review the Executive Subcommittee's recommendations for appointment and make such appointments as are consistent with 33 CFR 103.305, this charter, and the purpose of the Subcommittee. The Federal Maritime Security Coordinator will then conduct the required security background checks and extend letters of appointment to selected members.

Appointed members must indicate their intention to accept or decline the appointment and abide by the appointment as outlined in section 2344 of this charter, below. Members not accepting this appointment will return to general Port Security Committee membership status.

The Federal Maritime Security Coordinator will revoke any appointment at any time whenever he or she concludes such action is necessary for the efficient or effective functioning of the Executive Subcommittee, or when he or she concludes that the appointed member is not participating sufficiently to accomplish purposes of the Port Security Committees or the work of the Executive Subcommittee.

## **2344 Acceptance and Pledge**

Once nominated, qualified candidates accepted by the Federal Maritime Security Coordinator will be accepted as appointed members of the Executive Subcommittee by pledging to abide by the rules of this charter and to act in good faith and to the best of their ability in the application of the policies and procedures established by the Executive Subcommittee. Executive Subcommittee members shall indicate their adoption of this pledge by affixing to their appointment letter or a copy thereof the signature of both the member and his or her supervisor (where appropriate). The Subcommittee Member shall return a signed copy of the appointment letter to the Port Security Committee Co-Chairs. Subsequent intent by a member to withdraw from the Executive Subcommittee shall be conveyed to Co-Chairs through written notification. Appointed members are not authorized to deputize assistance or others to attend Port Security Meetings or Executive Subcommittee Meetings on their behalf; continuity of participation and fluency in the issues at hand will not permit this practice.

The Port Security Committee Co-Chairs shall periodically request the Executive Subcommittee review, and if necessary revise, the total numbers and composition of the Subcommittee. When changes are approved, the Co-Chairs will request nominations and make appointments as outlined in Section 2343 above.

## **2345 Officers of the Executive Subcommittee**

The Chair of the Executive Subcommittee for each Port Security Committee shall be elected by that Executive Subcommittee only, not by the body of the whole Port Security Committee, and shall be an appointed member of that Executive Subcommittee. The Chair shall appoint, with the consent of the Executive Subcommittee, a Secretary and a Chair for each of that PSC's Working Subcommittees from among the appointed members. The policies and procedures of the Port Security Committee, either by consensus or vote, shall be recorded and publicized by the Secretary. The Secretary shall also record and publish minutes of each Port Security Committee meeting and maintain a list of active PSC members. The Secretary shall also maintain a list of the Executive Subcommittee members. Officers shall retain voting privileges during their terms of service.

## **2346 Schedule of Meetings**

Each Executive Subcommittee shall meet at least once during each calendar year and preferably once each quarter. The time and venue of the meetings shall be determined by the Executive Subcommittee

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-11
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

Chair and members. Arrangements for these meetings shall be made by the Executive Subcommittee Chair. Annual and Quarterly meetings shall be open to the Port Security Committee and shall not cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information. The Executive Subcommittee Chair shall schedule meetings to cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information restricted to the appointed members and select expert invitees separately; rules governing those sessions are described in section 2351 below.

## 2347 Executive Subcommittee Procedural Rules

**Rule 1. Executive Subcommittee Policy.** It is the policy of the Executive Subcommittee that Port Security Committee members shall have the opportunity to speak to any Executive Subcommittee meeting agenda item before final action.

**Rule 2. Spokesperson for a Group of Persons.** When any group of persons wishes to address the Executive Subcommittee on the same subject matter, it shall be proper for the presiding officer to request that a spokesperson be chosen by the group to address the Subcommittee.

**Rule 3. Scheduling of Closed Session.** Bearing in mind section 2351 of this charter (below), special closed sessions shall be scheduled to the extent possible and appropriate prior to Port Security Committee membership meetings. Any closed session may be scheduled during or after a general Port Security Committee meeting.

**Rule 4. Meeting Adjourned to Date Certain.** When an Executive Subcommittee meeting is adjourned, it must in all cases be adjourned to another scheduled meeting date. All unfinished items will be listed in their original order after roll call on the agenda of such scheduled meeting.

**Rule 6. Agenda Matters.** The principle procedure for holding Executive Subcommittee meetings will be an agenda. All meetings shall have an agenda.

**Rule 7. Presiding officer to state issue.** The presiding officer shall assure that all issues are clearly stated before allowing discussion to begin. The presiding officer may also restate the issue before allowing discussion to continue or prior to voting.

**Rule 8. Presiding officer may discuss and vote.** The presiding officer may move, second and discuss from the chair, subject only to such limitations of debate as are by these rules imposed on all Executive Subcommittee members. The presiding officer shall not be deprived of any of the rights and privileges of a Subcommittee member.

**Rule 9. Quorum.** A majority of the committee membership shall constitute a quorum.

**Rule 10. Referrals.** Referrals to the working subcommittees shall be made by the Executive Subcommittee. Items may be withdrawn from the working subcommittee and taken up for consideration by the Executive Subcommittee at any meeting with the consent of a majority of the Executive Subcommittee members.

**Rule 11. Minutes.** The Executive Subcommittee shall not be required to prepare and distribute minutes of its meetings. Notes shall be taken by the Chair; these notes need not be verbatim but shall reflect the sense of the discussion and any recommendation made with

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-12
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

respect to each subject considered in subcommittee. Votes shall be formally recorded including the item voted upon and the total votes for and against. A report of the subcommittee shall be delivered to the Port Security Committee during its quarterly meetings and to the Federal Maritime Security Coordinator upon request.

**Rule 12. Conduct of Executive Subcommittee Meetings.** The chair of the Executive Subcommittee may conduct meetings with as much informality as is consistent with these charter procedural rules. The views of interested private citizens may be heard in certain subcommittee meetings, but in no case shall a subcommittee meeting be used as a substitute for the Port Security Committee meetings.

**Rule 13. Authorization to Vote.** Each appointed member of the Executive Subcommittee may have one vote; votes will not be apportioned according to agency, jurisdiction, or other criterion. With the prior approval of the Federal Maritime Security Coordinator and only in limited exceptional circumstances, a designated alternate may vote in place of an appointed member.

**Rule 14. Manner of Voting.** On the passage of every motion or recommendation to the Federal Maritime Security Coordinator, the vote shall be taken and a formal record of both the motion and votes for and against recorded.

**Rule 15. Silence constitutes affirmative vote.** Executive Subcommittee members who are silent during a voice vote shall have their vote recorded as an affirmative vote, except when individual appointed members have stated in advance that they will not be voting.

**Rule 16. Failure to vote.** It is the responsibility of every appointed Executive Subcommittee member to vote unless disqualified for cause. No appointed AMSC member can be compelled to vote.

**Rule 17. Abstaining from vote.** The abstainer chooses not to vote and, in effect, "consents" that a majority of the quorum of the executive subcommittee members present may act for him or her.

**Rule 18. Not participating.** An Executive Subcommittee member who disqualifies him or herself because of any financial or other interest in the issue at hand shall disclose the nature of the conflict and may not participate in the discussion or the vote. A member may otherwise disqualify him or herself due to personal bias or the appearance of impropriety.

**Rule 19. Tie votes.** Tie votes may be reconsidered on motion by any member of the Executive Subcommittee voting aye or nay during the original vote. Before a motion is made on the next item on the agenda, any member of the Executive Subcommittee may make a motion to continue the matter to another date. Nothing herein shall be construed to prevent any member from agendaizing a matter which resulted in a tie vote for a subsequent meeting.

## 2350 Handling and Protecting Information

Pursuant to Title 49 Code of Federal Regulations Part 1520, this part governs the release, by the Port Security Committee membership, and by other persons, of records and information that has been obtained or developed during security activities.

For purposes of this section, **Record** includes any writing, drawing, map, tape, film, photograph, or

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-13
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



other means by which information is preserved, irrespective of format. **Vulnerability assessment** means any examination of a transportation system, vehicle, or facility to determine its vulnerability to unlawful interference.

Port Security Committee members must restrict disclosure of and access to sensitive security information described in this section to persons with a need to know and must refer requests by other persons for such information to Coast Guard Federal Maritime Security Coordinator.

**Need to know.** For some specific sensitive security information, the Federal Maritime Security Coordinator may make a finding that only specific persons or classes of persons have a need to know. Otherwise, a person has a need to know sensitive security information in each of the following circumstances:

- (1) When the person needs the information to carry out approved, accepted, or directed security duties.
- (2) When the person is in training to carry out approved, accepted, or directed security duties.
- (3) When the information is necessary for the person to supervise or otherwise manage the individuals carrying out approved, accepted, or directed security duties.
- (4) When the person needs the information to advise persons regarding any DHS/DOT security-related requirements.
- (5) When the person needs the information to represent the persons listed in paragraph (1) of this section in connection with any judicial or administrative proceeding regarding those requirements.

**Release of sensitive security information.** When sensitive security information is released to unauthorized persons, any Port Security Committee member or individual with knowledge of the release, must inform the Coast Guard Federal Maritime Security Coordinator.

**Violation.** Violation of these rules is grounds for a civil penalty and other enforcement or corrective action.

**These rules will be followed to protect all Security Sensitive Information, Commercial Sensitive Information, and Proprietary Information. Classified Material will be protected in accordance with the rules governing it.**

## 2351 Rules for SSI Sessions & SSI Information

**Rule 1. Authorized Closed Sessions.** Subject to the advice of the Federal Maritime Security Coordinator and the requirements of 49 CFR Part 1520, closed sessions may generally be held to discuss the following subjects:

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-14
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

(1) Security matters, i.e., matters posing a threat to the public's right of access to public services or public facilities, as outlined in 49 CFR Section 1520.7, including Security Sensitive Information portions of the Area Maritime Security Assessment and AMS Plan.

(2) Pending litigation and administrative proceedings prosecuted by or against the Federal Maritime Security Coordinator or Port Security Committees, including but not limited to settlement proceedings.

(3) Other closed sessions authorized by the Federal Maritime Security Coordinator.

**Rule 2. Calling Closed Sessions.** Subject to the advice of the Federal Maritime Security coordinator, a closed session may be called by the Port Security Committee Co-Chairs or by the Executive Subcommittee.

Closed sessions shall be noticed on the agenda. To the greatest extent possible, the Federal Maritime Security Coordinator and PSC Co-chairs shall use standardized agenda descriptions that are consistent with 49 CFR part 1520.7.

The Port Security Committee shall convene in open session and provide an opportunity for general membership comment as to the closed session items before any closed session. The Co-chairs shall be present in the open session to record any statements made. The Co-Chairs shall announce the item or items to be considered in closed session by reference to the appropriate agenda item, or in an alternate form provided by the Federal Maritime Security Coordinator.

**Rule 3. Attendance at Closed Sessions.** The Co-Chairs, or their designees, shall attend closed sessions unless it is necessary to excuse them. Only such additional staff shall attend as are necessary and then only if the legal privileges of confidentiality obtained in an executive session are not waived.

**Rule 4. Reports from Closed Session.** It is the policy of the Port Security Committees to inform the public of action taken in closed session to the greatest extent possible. It is recognized, however, that the need for confidentiality is inherent in closed sessions and that certain matters if revealed may be a detriment to the results desired.

Reports from closed sessions, when permissible, shall be made by Co-Chairs or such other representative as designated by the Executive Subcommittee. Such designated person is the only individual authorized to make public statements concerning the closed session.

**Rule 5. Record of Disclosure of Security Sensitive Information.** The Co-Chairs shall assure that appropriate records are retained regarding the disclosure of SSI on a need to know basis, the specific Port Security Committee members to whom the information was disclosed, and the date.

## 2352 Rules for Classified Sessions & Classified Information

Classified Information must be protected under the rules governing it. Those rules shall be adhered to in all respects during classified sessions of the Port Security Committee. To the extent practicable, the rules outlined in section 2351 shall also be adhered to.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-15
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 2353 Rules for Commercially Sensitive Information

Commercially Sensitive Information must also be protected. In all cases, Commercially Sensitive Information shall be treated in similar fashion to Security Sensitive Information and the rules outlined in section 2351 shall be adhered to.

## 2354 Rules for Proprietary Information

Proprietary Information must also be protected. In all cases, Proprietary Information shall be treated in similar fashion to Security Sensitive Information and the rules outlined in section 2351 shall be adhered to.

## 2360 Amending The Charter

This charter may be amended at any time by the Port Security Committee Co-Chairs. Recommendations to the Co-Chairs for changes to this charter may be made only with the approval of two-thirds of the Executive Subcommittee members.

## 2400 Relationship to Other Committees

The AMS Committee consults on an as-needed basis with the following other planning and preparedness committees:

- **The Jacksonville Port Readiness Committee (JPRC).** The Jacksonville Port Readiness Committee is a standing, chartered committee comprised of those entities with governmental or commercial contractual responsibilities in preparing the Port of Jacksonville for major Department of Defense military logistical outload as a Sea Port of Embarkation (SPOE). The Military Sealift Command, Jacksonville Port Authority, U.S. Coast Guard, Military Traffic Management Command, CSX Railroad, Florida Highway Patrol, and the Department of Transportation Maritime Administration (MARAD) are the major participants. The JPRC is chaired by the Coast Guard Captain of the Port/Federal Maritime Security Coordinator. The Port Security Committees consult with the JPRC in planning and providing security in the port and at military outload sites (commercial property) for mobilizations.
- **The Jacksonville Maritime Transportation Exchange (JMTX).** The Jacksonville Maritime Transportation Exchange is a Local Coordination Council under the Marine Transportation System (MTS) initiative co-sponsored by the U.S. Coast Guard and the Department of Transportation Maritime Administration. The MTS initiative and JMTX seek to responsibly develop the procedural and physical infrastructure to allow the projected doubling of maritime commerce by the year 2020. JMTX sponsors and facilitates the meeting of all government and private interests for the purpose of identifying and eliminating obstacles to this expansion and redundancies possibly affecting Jacksonville as the Atlantic seaboard port of choice.
- **The JMTX Harbor Safety Committee (HSC).** JMTX and U.S. Coast Guard sponsor the harbor safety committee for the port of Jacksonville. The harbor safety committee's mission is to identify unsafe conditions and operations in the port of Jacksonville, then bring government and private entities together to maintain the level of safety in the port.
- **The Area Planning Committee (APC).** The Area Planning Committee is a voluntary participation committee composed of governmental response agencies and private spill response entities including contractors and facility owners. The APC's purpose is to advise the Coast Guard and Environmental Protection Agency in the preparation of the Area Contingency Plan under Title 40 CFR 300, a plan which governs all agencies in the response to oil and hazardous material spills/releases in the Northeast and Eastern Central Florida area. This plan includes specific guidance regarding marine firefighting and response to Weapons of

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-16
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

Mass Destruction.

- **The Northeast Florida Regional Planning Council (NEFRPC).** The Northeast Florida Regional Planning Council (NEFRPC) is a dynamic network of local governance, serving seven counties - Baker, Clay, Duval, Flagler, Putnam, Nassau and St. Johns – and their 27 municipalities. NEFRPC's mission is: To provide visionary leadership and coordination between counties and governmental agencies to preserve and enhance the quality of Northeast Florida's natural, man-made, economic, and social environment. The Council accomplishes this mission by:
  - Actively serving as a convenor of regional issues,
  - Building consensus for regional solutions through coordination and cooperation,
  - Providing a regionally focused forum for comprehensive and functional planning,
  - Furnishing technical and administrative assistance to local governments and other stakeholders,
  - Fostering public awareness of diverse regional issues,
  - Maintaining expertise among staff and pursuing technologies that support the successful implementation of the mission,
  - Identifying trends, issues and opportunities for the region.

Regional Planning Councils are authorized by Florida Statutes. There are 11 [Regional Planning Councils](#) in the state of Florida.

- **Eastern Central Florida Regional Planning Council (ECFRPC).** The ECFRPC region encompasses the urban centers of Orlando, Daytona Beach, DeLand, Melbourne, Kissimmee, Leesburg and Sanford, the Kennedy Space Center and the Walt Disney World vacation area. It is the mission of the Eastern Central Florida Regional Planning Council to work with communities in expanding and enhancing these abilities, and, in doing so, connect with one another in planning their shared future. The Regional Planning Council approaches its mission through an array of programs and projects. The mix of activities changes from year to year depending upon community needs, but all projects and programs fall within one or more of the following categories: Planning Tools, Planning Techniques, Information Development, Regional Leadership Training and Education, Organizational Partnerships, and Regional Coalitions and Compacts.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	2000-17
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## 3000 (U) AWARENESS

This section of the AMS Plan details how rapid access to vital information will be given to Northeast and Eastern Central Florida critical decision makers during routine and crisis maritime situations. The section is organized as follows:

3100	<u>Introduction</u>
3200	<u>Federal, State &amp; Local Security and Law Enforcement Agency Jurisdiction</u>
3300	<u>Area Maritime Security Assessment</u>
3400	<u>Communications</u>
3500	<u>Sensitive Security Information</u>
3600	<u>Maritime Security Training</u>
3700	<u>Maritime Security Resources</u>

## 3100 (U) Introduction

The AMS Plan is the fundamental element in building vigilant “Situational Awareness” and is key to the successful development of the Maritime Domain Awareness program. It will serve to assist the United States Department of Homeland Security in producing a “common operations picture” (COP) of the maritime environment. The AMS Plan affords rapid access to vital information by critical decision makers within the area maritime community during routine and crisis maritime situations.

## 3200 (SSI) Law Enforcement Agency Jurisdiction

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 3300 (U) Area Maritime Security (AMS) Assessment

This Area Maritime Security Assessment is organized as follows:

3310	<u>Introduction</u>
3320	<u>Critical Marine Transportation Infrastructure and Operations</u>
3330	<u>Area Maritime Security Threat Assessment</u>
3340	<u>Area Maritime Security Assessment</u>
3350	<u>Security Measures for MARSEC 1, 2, and 3</u>
9400	<u>Appendices</u>

## 3310 (U) Introduction

The Port Security Committees for the Northeast and Eastern Central Florida have created this Area Maritime Security Assessment (AMSA) to provide strategies, tactics, techniques, and procedures for the protection and defense of the United States Marine Transportation System (MTS) from smuggling, thievery, illegal protest, and terrorism. This AMSA has been undertaken in accordance with requirements of Title 33 Code of Federal Regulations part 103 and the guidance in Coast Guard Navigation and Vessel Inspection Circular 11-02. This section and the Area Maritime Security Assessment are Sensitive Security Information in accordance with section 3500 of this plan and must be so protected in their entirety.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-1
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

This AMS Plan was based on the AMS Assessment, which is a risk-based analysis of Northeast and Eastern Central ports and waterways. The general steps in this process were:

- 1) Identifying critical operations and infrastructure;
- 2) Selecting a list of credible, analyzable attack scenarios;
- 3) Conducting threat, consequence and vulnerability assessments for each scenario;
- 4) Categorizing and prioritizing scenarios with unacceptably high risk for action; and
- 5) Designing security measures controlling those scenarios to acceptable levels.

## **3320 (SSI) Critical Marine Transportation Infrastructure and Operations**

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## **3330 (SSI) Area Maritime Security Threat Assessment**

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## **3340 (SSI) Area Maritime Security Assessment**

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## **3350 (SSI) Security Measures for MARSEC 1, 2, and 3**

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## **3400 (U) Communications**

Effective communications is vital to pre- and post incident response. An understanding of communications methodology, programs, processes, and physical attributes is essential to all personnel involved in the security process.

The AMS Plan must identify how and when the Committee will meet if called upon to advise and assist the FMSC in the communication of security information, what kind of assistance it will provide, and how it will provide it.

The AMS Plan must also identify redundant methods for communicating vital information to ensure all appropriate facilities, vessels, maritime stakeholders, and recreational boaters are notified.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-2
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



The AMS Plan should address the benefits of communicating with the public, and the value of establishing programs similar to neighborhood watch programs. Programs of this nature have been found to be very beneficial in raising public awareness and involving the community in enhancing security. Further guidance is under development to assist FMSCs in developing community awareness programs that will encourage community reporting suspicious activities and behavior.

This section outlines the means by which communication under this plan will occur. The section is organized as follows (click the link to view the subsection):

- 3410 Communication of Security Information
  - 3410.1 Communication with the General Public
  - 3410.2 Communication with Waterway Users (Boaters)
  - 3410.3 Communication with Commercial Vessels
  - 3410.4 Communication with Commercial Shoreline Facilities
  - 3410.5 Communication with Companies
  - 3410.6 Role of the Port Security Committees in Communicating Security Information
- 3420 Security Reporting
  - 3420.1 Procedures for Reporting Suspicious Activity
  - 3420.2 Procedures for Reporting Breaches in Security
  - 3420.3 Procedures for Reporting a Transportation Security Incident
- 3430 Communicating MARSEC Directives
  - 3430.1 Procedures for Communicating MARSEC Directives
  - 3430.2 Procedures for Responding to MARSEC Directives
  - 3430.3 Role of the Port Security Committees in Communicating MARSEC Directives
- 3440 Communicating MARSEC Levels
  - 3440.1 Procedures to Communicate Changes in MARSEC Levels
  - 3440.2 Notification of MARSEC Level Attainment
  - 3440.3 Role of the Port Security Committee in Communicating MARSEC Levels

## 3410 (U) Communication of Security Information

Security informational needs are multilayered with a large variety of stakeholder requirements or needs. The next sections will identify methodology used to communicating security information.

The Port Security Committees and the Maritime Joint Task Force have developed a communication plan using the P-A-C-E method. This method can be used for routine or crisis situations and will be tested periodically to ensure connectivity.

- P** Primary system of contact for disseminating information.
- A** Alternate system of contact (can be same method as primary but on a different frequency or phone number).
- C** Contingency system is used when both the primary and alternate are not effective.
- E** Emergency is the most failsafe and should be used in a real emergency or when the other systems are not successful.

Section 3500 of this plan contains information pertaining to the protection and dissemination of SSI.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-3
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3410.1 (U) Communication with the Public

The public as whole must be notified of events and operations that might affect them. There are a variety of systems that may be used to communicate information on restrictions, closures, and activities that are exclusionary or restrictive in nature.

**Table 3410.1-1: (U) Communication to the General Public**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Homeland Security Advisory System (HSAS) Threat Advisory Level and specific waterway closures linked to the HSAS Threat Level.	Department of Homeland Security	<b>P</b> - Via major media outlets.	Within DHS-established timeframes related to the decision to change the HSAS level.
	Coast Guard Integrated Command Center	<b>A</b> - Through electronic distribution of a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages; a volunteer subscription list is contained in <a href="#">Tab G to Appendix 9500</a> – interested waterway users may subscribe or delete their addresses from this list on a continuous basis. See <a href="#">Tab (H) to Appendix 9500</a> .	Within 2 Hours of MARSEC level changes and associated waterway closures.
	Coast Guard Integrated Command Center	<b>C</b> - Recurring Broadcast Notice to Mariners issued on Channel 16. See <a href="#">Tab N to Appendix 9500</a> .	Within 2 Hours of MARSEC level changes and associated waterway closures.
	County Emergency Operations Centers	<b>E</b> - Emergency evacuation/alert phone calls and Emergency Broadcast System alerts.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
Marine and Special Shoreline Event restrictions that could bear on attendees.	USCG MSO Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the <a href="#">4000 Series – PREVENTION</a> .	Not later than 01 July 2004 and updated at least annually.
	USCG MSO Jacksonville	<b>A</b> - Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	<b>C</b> - Periodic Broadcast Notice to Mariners issued on Channel 16. See <a href="#">Tab N to Appendix 9500</a> .	Within Two Hours of set of higher MARSEC Levels. Additionally within one hour of Marine Events controlled by the Area Maritime Security Plan.
	MJTF Law Enforcement Vessels	<b>E</b> - Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels.	During escort and patrol activities afloat.
Evacuation instructions linked to credible threats and/or Transportation Security Incidents that could affect large residential/high-occupancy areas.	County Emergency Operations Centers	<b>P</b> - Emergency evacuation/alert phone calls.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
	County Emergency Operations Centers	<b>A</b> - Emergency Broadcast System alerts and media releases.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
	Coast Guard Integrated Command Center	<b>C</b> - Text/Page call to FSO's/VSO's/CSO's.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
	Coast Guard Integrated Command Center	<b>E</b> - Periodic Broadcast Notice to Mariners issued on Channel 16. See <a href="#">Tab N to Appendix 9500</a> .	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-4
--------------	--------------------	-------------------------------	-----------------------	--------------	-------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3410.1-1: (U) Communication to the General Public (continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Incident specific information detailing the nature of the incident and the level of terrorist threat indicated by the incident.	Department of Homeland Security	<b>P</b> - Via major media outlets.	Within DHS-established timeframes related to the decision to change the HSAS level.
	Federal Maritime Security Coordinator	<b>A</b> - Through Press Releases and statements to the public regarding Coast Guard activities.	Within 24 hours of the incident.
	JMTX Port Security Committee and Port Canaveral Security Committee	<b>C</b> - During emergency Port Security Committee meetings.	Where information and press interest warrants
	MJTF Law Enforcement Ashore and Afloat	<b>E</b> - Delivery of appropriate threat info to specific areas, vessels, facilities, and individuals	In extreme emergencies when the SSI incident specific information must be directly provided in order to protect lives, as soon as possible.
Suspicious Activity, Security Breach, and Transportation Security Incident Response Procedures for non-governmental entities to follow (at the unclassified level).	U.S. Coast Guard MSO Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the 9000 Annex for "green sheet" unclassified procedures.	Not later than 01 July 2004 and updated at least annually.
	JMTX Port Security Committee and Port Canaveral Security Committee	<b>A</b> - Through Port Security Committee educational campaigns aimed at the larger waterway community.	Starting not later than 01 July 2004 and repeated at least annually.
	U.S. Coast Guard MSO Jacksonville	<b>C</b> - Through production of publicly available "greensheet" procedure extracts.	As soon as possible following 01 July 2004.
	MJTF Law Enforcement Ashore and Afloat	<b>E</b> - Delivery of appropriate specific instructions to specific areas, vessels, facilities, and individuals	In extreme emergencies when the SSI incident specific information must be directly provided in order to protect lives, as soon as possible.

**Table 3410.1-2: (U) Communication from the General Public**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Reports of Suspicious Activity.	Any member of the general public.	<b>P</b> - To the Coast Guard Integrated Command Center (dial <b>904-247-7318</b> ) and the National Response Center (dial <b>800-424-8802</b> )	<b>24/7</b> - As soon as possible upon observing suspicious activity.
		<b>A</b> - To local law enforcement (dial <b>911</b> ) - request the information be relayed to the Coast Guard.	<b>24/7</b> - As soon as possible upon observing suspicious activity.
		<b>C</b> - To the Coast Guard Integrated Command Center via Fax at 904-247-7371, Voice 904-247-7318 and Cell 904-334-7697.	<b>24/7</b> - As soon as possible upon observing suspicious activity.
		<b>E</b> - To the Coast Guard Integrated Command Center via VHF Radio ( <b>Channel 16</b> ).	<b>24/7</b> - As soon as possible upon observing suspicious activity.
Reports of Security Breaches and/or apparent Transportation Security Incidents.	Any member of the general public.	<b>P</b> - To local law enforcement (dial <b>911</b> ), to the Coast Guard Integrated Command Center (dial <b>904-247-7318</b> ) and the National Response Center (dial <b>800-424-8802</b> )	<b>24/7</b> - As soon as possible upon observing the incident or evidence of a security breach.
		<b>A</b> - To the Coast Guard Integrated Command Center via Fax at 904-247-7371, Voice 904-247-7318 and Cell 904-334-7697.	<b>24/7</b> - As soon as possible upon observing the incident or evidence of a security breach.
		<b>C</b> - To the Seventh Coast Guard District Command Center at <b>305-415-6800</b> .	<b>24/7</b> - As soon as possible upon observing the incident or evidence of a security breach.
		<b>E</b> - To the Coast Guard Integrated Command Center via marine band VHF Radio ( <b>Channel 16</b> ).	<b>24/7</b> - As soon as possible upon observing the incident or evidence of a security breach.

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS/SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>NE FL SECTOR</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>3000-5</b>
---------------------	----------------------------	---	------------------------------	---------------------	--------------------------	-----------------------------	-------------	---------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3410.1-2: (U) Communication from the General Public (Continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Complaints regarding lack of security, security measures, impact on the general public, or the professionalism of security personnel.	Any member of the general public.	<b>P</b> - In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	<b>24/7</b> - As soon as possible
		<b>A</b> - Using the USCG Marine Safety Office Jacksonville web page electronic complaint submission form.	<b>24/7</b> - As soon as possible
		<b>C</b> - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office - (click here for driving directions).	<b>24/7</b> - As soon as possible
		<b>E</b> - Telephone to the USCG MSO Jacksonville Port Preparedness Department, 904-232-2640 x104.	During working hours between 0730 a.m. and 1600 p.m. weekdays.
Input on this Area Maritime Security Plan.	Any member of the general public.	<b>P</b> - In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	<b>24/7</b> - As soon as possible
		<b>A</b> - Using the USCG Marine Safety Office Jacksonville web page electronic comment submission form. ( <a href="http://www.uscg.mil/d7/units/mso-jax/Readiness &amp; Preparedness/Area_maritime_Security_comments.htm">http://www.uscg.mil/d7/units/mso-jax/Readiness &amp; Preparedness/Area_maritime_Security_comments.htm</a> )	<b>24/7</b> - As soon as possible
		<b>C</b> - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office - (click here for driving directions).	<b>24/7</b> - As soon as possible
		<b>E</b> - Telephone to the USCG MSO Jacksonville Port Preparedness Department, 904-232-2640 x111.	During working hours between 0730 a.m. and 1600 p.m. weekdays.

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS/SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>NE FL SECTOR</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>3000-6</b>
---------------------	----------------------------	---	------------------------------	---------------------	--------------------------	-----------------------------	-------------	---------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3410.2 (U) Communications with Waterway Users (Boaters)

Communicating security information to waterway users includes many of the processes currently used to identify hazards to navigation or safety related concerns on the MTS.

**Table 3410.2-1: (U) Communication to Waterway Users**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Maritime Security (MARSEC) level and specific waterway closures linked to the MARSEC level.	Coast Guard Integrated Command Center	<b>P</b> - Through optional text page and electronic distribution of a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages; a volunteer subscription list is contained in <a href="#">Tab G to Appendix 9500</a> – interested waterway users may subscribe or delete their addresses from this list on a continuous basis. See Tab G to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
		<b>A</b> – Through fax distribution of the same Marine Safety Information Bulletin to entities on the volunteer subscription list.	Within 8 Hours of MARSEC level changes and associated waterway closures.
		<b>C</b> - Recurring Broadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> – Posting of notices in marinas, yacht clubs, tackle and bait stores, and marine supply shops.	Only when electronic, fax and radio distribution systems are not functional and/or deemed inadequate due to insufficient subscription.
Moving security zones around vessels. Fixed security zones and USACE restricted areas in the Area.	Coast Guard Marine Safety Office Jacksonville and the Government Printing Office (GPO)	<b>P</b> - Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	USCG MSO Jacksonville	<b>A</b> – Graphic diagrams of restricted areas and security zones posted on the Marine Safety Office Jacksonville, Group Mayport, JMTX, and Canaveral Port Authority web pages	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	<b>C</b> - Periodic Broadcast Notice to Mariners issued on Channel 16. See Tab N to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels.
	MJTF Law Enforcement Vessels	<b>E</b> – Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels.	During escort and patrol activities afloat.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-7
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3410.2-1: (U) Communication to Waterway Users (continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Marine Event participation instructions and security restrictions	USCG MSO Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the 4000 Series – PREVENTION.	Not later than 01 July 2004 and updated at least annually.
	USCG MSO Jacksonville	<b>A</b> – Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	<b>C</b> - Periodic Broadcast Notice to Mariners issued on Channel 16. See Tab N to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels. Additionally within one hour of Marine Events controlled by the Area Maritime Security Plan.
	MJTF Law Enforcement Vessels	<b>E</b> – Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels.	During escort and patrol activities afloat.
Specific security measures all members of the maritime public are expected to execute at each MARSEC Level.	USCG Marine Safety Office Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the 4000 Series – PREVENTION.	Not later than 01 July 2004 and updated at least annually.
	USCG MSO Jacksonville	<b>A</b> – Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	<b>C</b> - Periodic Broadcast Notice to Mariners issued on Channel 16. See Tab N to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels.
	MJTF Law Enforcement Ashore and Afloat	<b>E</b> – Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels, facilities, and individuals	During security, escort and patrol activities afloat and ashore.
Suspicious Activity, Security Breach, and Transportation Security Incident Response Procedures for non-governmental entities to follow (at the unclassified level).	U.S. Coast Guard MSO Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the 9000 Annex for "green sheet" unclassified procedures.	Not later than 01 July 2004 and updated at least annually.
	JMTX Port Security Committee and Port Canaveral Security Committee	<b>A</b> - Through Port Security Committee educational campaigns aimed at the larger waterway community.	Starting not later than 01 July 2004 and repeated at least annually.
	U.S. Coast Guard MSO Jacksonville	<b>C</b> - Through production of publicly available "greensheet" procedure extracts.	As soon as possible following 01 July 2004.
	MJTF Law Enforcement Ashore and Afloat	<b>E</b> – Delivery of appropriate specific instructions to specific areas, vessels, facilities, and individuals	In extreme emergencies when the SSI incident specific information must be directly provided in order to protect lives, as soon as possible.

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS/SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>NE FL SECTOR</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>3000-8</b>
---------------------	----------------------------	---	------------------------------	---------------------	--------------------------	-----------------------------	-------------	---------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



**Table 3410.2-2: (U) Communication from Waterway Users**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Reports of Suspicious Activity.	Any waterway user or boater	<b>P</b> - To the Coast Guard Integrated Command Center (dial <b>904-247-7318</b> ) and the National Response Center (dial <b>800-424-8802</b> )	As soon as possible upon observing suspicious activity.
		<b>A</b> - To local law enforcement (dial <b>911</b> ) - request the information be relayed to the Coast Guard.	As soon as possible upon observing suspicious activity.
		<b>C</b> - To the Coast Guard Integrated Command Center via Fax at 904-247-7371, Voice 904-247-7318 and Cell 904-334-7697.	As soon as possible upon observing suspicious activity.
		<b>E</b> - To the Coast Guard Integrated Command Center via VHF Radio ( <b>Channel 16</b> ).	As soon as possible upon observing suspicious activity.
Reports of Security Breaches and/or apparent Transportation Security Incidents. Reports of Hazards to Navigation.	Any waterway user or boater	<b>P</b> - To local law enforcement (dial <b>911</b> ), to the Coast Guard Integrated Command Center (dial <b>904-247-7318</b> ) and the National Response Center (dial <b>800-424-8802</b> )	As soon as possible upon observing the incident or evidence of a security breach.
		<b>A</b> - To the Coast Guard Integrated Command Center via Fax at 904-247-7371, Voice 904-247-7318 and Cell 904-334-7697.	As soon as possible upon observing the incident or evidence of a security breach.
		<b>C</b> - To the Seventh Coast Guard District Command Center at <b>305-415-6800</b> .	As soon as possible upon observing the incident or evidence of a security breach.
		<b>E</b> - To the Coast Guard Integrated Command Center via VHF Radio ( <b>Channel 16</b> ).	As soon as possible upon observing the incident or evidence of a security breach.
Complaints regarding lack of security, security measures, impact on the general public, or the professionalism of security personnel.	Any waterway user or boater	<b>P</b> - In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	As soon as possible
		<b>A</b> - Using the USCG Marine Safety Office Jacksonville web page electronic complaint <a href="#">submission form</a> .	As soon as possible
		<b>C</b> - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office - (click here for driving directions).	As soon as possible
		<b>E</b> - Telephone to the USCG MSO Jacksonville Port Preparedness Department, <b>904-232-2640 x104</b> .	During working hours between 0730 a.m. and 1600 p.m. weekdays.
Input on this Area Maritime Security Plan.	Any waterway user or boater	<b>P</b> - In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	As soon as possible
		<b>A</b> - Using the USCG Marine Safety Office Jacksonville web page electronic comment submission form at <a href="http://www.uscg.mil/units/web">www.uscg.mil/units/web</a> address].	As soon as possible
		<b>C</b> - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office - (click here for driving directions).	As soon as possible
		<b>E</b> - Telephone to the USCG MSO Jacksonville Port Preparedness Department, <b>904-232-2640 x104</b> .	During working hours between 0730 a.m. and 1600 p.m. weekdays.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-9
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3410.3 (U) Communications with Commercial Vessels

Communicating with commercial vessels will require a number of systems that will provide linkages to the large variety of vessels operating within the MTS.

**Table 3410.3-1: (U) Communication to Commercial Vessels**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Security information relevant to a single vessel.	Coast Guard Integrated Command Center	<b>P</b> - Through text page or direct phone contact to the Vessel and Company Security Officer.	As soon as possible after obtaining the security information relevant to a single vessel.
		<b>A</b> - Through the vessel's shipping agents and the bar pilots, relaying the message that the vessel is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officer confirms he/she cannot make timely contact with the vessel to communicate the information directly.
		<b>C</b> - Through VHF radio contact with the vessel requiring the vessel to make direct land-line contact with the Coast Guard Integrated Command Center.	When the CSO confirms he/she cannot make timely contact.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Activation of the vessel's GMDSS receiver. Search, location, and delivery in person of appropriate security information to the Vessel Security Officer	Only when all other means of reaching the vessel have failed.
Security information relevant to an entire class or type of vessel (common trade, common ownership, common country-of-origin, etc.)	Commandant of the Coast Guard	<b>P</b> - Issuance of a MARSEC Directive and publishing notice of that issuance in the Federal Register.	As soon as possible after obtaining the security information relevant to a class of vessels.
	Coast Guard Integrated Command Center	<b>A</b> - Through a limited access meeting to distribute Directives - electronic distribution of a notification text page to VSO's and CSO's via e-mail about the meeting. Through direct phone contact to the Vessel and Company Security Officers. See <u>Tab A and C to Appendix 9500</u>	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of vessels.
		<b>C</b> - Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Vessel Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information
		<b>E</b> - Through direct phone contact to the Vessel and Company Security Officer.	As soon as possible after obtaining the security information relevant to a class of vessels.
Security information relevant to all commercial vessels (regardless of class or type) within a given geographic region or area.	Coast Guard Integrated Command Center	<b>P</b> - Through a limited access meeting to distribute Directives - electronic distribution of a notification text page to VSO's and CSO's via e-mail about the meeting. Through direct phone contact to the Vessel and Company Security Officers. See <u>Tab A and C to Appendix 9500</u> .	As soon as possible after obtaining the security information
		<b>A</b> - Through vessel shipping agents and the bar pilots, relaying the message that the vessel is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officers confirm they cannot make timely contact with the vessels to communicate the information directly.
		<b>C</b> - Through VHF radio contact with the vessels requiring them to make direct land-line contact with the Coast Guard Integrated Command Center.	When the CSO confirms he/she cannot make timely contact..
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Activation of the vessels' GMDSS receiver. Search, location, and delivery in person of appropriate security information to the Vessel Security Officer	Only when all other means of reaching the vessels have failed.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-10
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Table 3410.3-1: (U) Communication to Commercial Vessels (continued)			
Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Suspicious Activity, Security Breach, and Transportation Security Incident Response Procedures for non-governmental entities to follow (at the unclassified level).	U.S. Coast Guard MSO Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the 9000 Annex for "green sheet" unclassified procedures.	Not later than 01 July 2004 and updated at least annually.
	JMTX Port Security Committee and Port Canaveral Security Committee	<b>A</b> - Through Port Security Committee educational campaigns aimed at the larger waterway community.	Starting not later than 01 July 2004 and repeated at least annually.
	U.S. Coast Guard MSO Jacksonville	<b>C</b> - Through production of publicly available "greensheet" procedure extracts.	As soon as possible following 01 July 2004.
	MJTF Law Enforcement Ashore and Afloat	<b>E</b> - Delivery of appropriate specific instructions to specific areas, vessels, facilities, and individuals	In extreme emergencies when the SSI incident specific information must be directly provided in order to protect lives, as soon as possible.
Department of Homeland Security Threat Information Bulletins, either at the unclassified level or at the SSI level.	Coast Guard Integrated Command Center	<b>P</b> - Through an unencrypted e-mail or fax to VSOs and CSOs deemed to have a need to know in the opinion of the Federal Maritime Security Coordinator. Where the bulletin is SSI, through an encrypted e-mail in accordance with Section 3590 of this plan. See <u>Tabs A and C to Appendix 9500</u> .	As soon as possible after obtaining the DHS Directive
		<b>A</b> - Through vessel shipping agents and the bar pilots, relaying the message that the vessel is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officers confirm they cannot make timely contact with the vessels to communicate the bulletin directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>C</b> - Through VHF radio contact with the vessels requiring them to make direct land-line contact with the Coast Guard Integrated Command Center.  <b>E</b> - Activation of the vessels' GMDSS receiver. Search, location, and delivery in person of appropriate security information to the Vessel Security Officer	When the CSO confirms he/she cannot make timely contact..  Only when all other means of reaching the vessels have failed.

See Tab B to Appendix 9500 for detailed points of contact.

Verification of receipt of information from Commercial Vessels is required only for communication of specific threats, MARSEC Directives, and MARSEC level changes. The procedures for acknowledging receipt of this information and for verifying attainment of directed security levels and measures can be found in section 3420 and 3430 of this plan.

#### Ship Security Alert System Communications

SOLAS Regulation XI-2/6 requires certain vessels to be outfitted with a ship security alert system (SSAS), which allows the vessel to covertly signal a competent authority that the security of the ship is under threat or has been compromised. Contracting Governments of foreign flagged vessels are required to immediately forward all SSAS transmissions from vessels within, or bound for, U.S. waters to the U.S. Coast Guard. At this time, notifications to federal, state and local law enforcement agencies will be the primary response to a ship security alert.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-11
--------------	--------------------	-------------------------------	-----------------------	--------------	-------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

In the event the Coast Guard receives a SSAS alert from a vessel, whether in the port or at sea, that alert will immediately be routed to the Coast Guard Marine Integrated Command Center for action. The ICC will notify the FBI, Customs and Border Protection, Immigration and Customs Enforcement and specific Tier I and Tier II agencies (listed in Section 3200) based on vessel location/law enforcement jurisdiction. When the vessel is moored in port, the cognizant Facility Security Officer will also be notified of the alert. Simultaneous with these alert notifications, the ICC will contact the vessel's Company Security Officer for an explanation of the nature of the SSAS alert. When sufficient information has been gathered, the FMSC will respond to the alert as a legitimate mis-activation, a report of suspicious activity, a security breach, or a transportation security incident as the situation dictates.

In concert with the Company Security Officer, the FMSC will treat claims of accidental or unexplainable SSAS activation as a possible Transportation Security Incident (TSI) and will respond as outlined in section 5200 of this plan, understanding that the claim of accidental SSAS activation may well be truthful. The ICC will work closely with the above named agencies to ensure appropriate unified action is undertaken or to cancel the initial alert.

The following are additional existing and proposed systems are central to successful communication with commercial vessels:

:

**Rescue 21.** Rescue 21 will ensure continuous, enhanced radio coverage out to 20 nautical miles from shore. Rescue 21 is powerful enough to capture the low-powered (1-watt) marine radios transmitting from 20 nautical miles offshore. Higher-powered radios may be captured even farther offshore.

**The Global Maritime Distress and Safety System (GMDSS).** The GMDSS is an internationally established communications, distress and safety system, which provides automatic identification of a caller and the location of a vessel in distress.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-12
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3410.4 (U) Communications with Facilities

Communication of security information with regulated and non-regulated facilities will be undertaken using prearranged methods similar to communication procedures and methods identified in individual facility security plans.

**Table 3410.4-1: (U) Communication to Commercial Shoreline Facilities**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Security information relevant to a single commercial shoreline facility.	Coast Guard Integrated Command Center	<b>P</b> - Through direct phone contact to the Facility Security Officer.	As soon as possible after obtaining the security information relevant to a single facility.
		<b>A</b> - Through direct phone contact to the Company Security Officer.	As soon as possible after obtaining the security information relevant to a single facility.
		<b>C</b> - Through the facility's neighbors and landlords, relaying the message that the FSO is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officer confirms he/she cannot make timely contact with the facility to communicate the information directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Hand delivery of appropriate security information to the Facility Security Officer	Only when all other means of reaching the facility have failed.
Security information relevant to an entire class or type of commercial shoreline facility (common trade, common ownership, common vessel-callers, etc.)	Coast Guard Integrated Command Center	<b>P</b> - Through a limited access meeting to distribute Directives - electronic distribution of a notification text page to VSO's and CSO's via e-mail about the meeting. Through direct phone contact to the Vessel and Company Security Officers. See <a href="#">Tabs A and C to Appendix 9500</a>	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of facilities.
		<b>A</b> - Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Facility Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		<b>C</b> - Through direct phone contact to the Facility and Company Security Officer.	As soon as possible after obtaining the security information relevant to a class of facilities.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Hand delivery of appropriate security information to the Facility Security Officer and Company Security Officer.	Only when all other means of reaching the facility have failed.
Security information relevant to all commercial shoreline facilities (regardless of class or type) within a given geographic region or area.	Coast Guard Integrated Command Center	<b>P</b> - Through a limited access meeting to distribute Directives - electronic distribution of a notification text page to FSO's and CSO's via e-mail about the meeting. Through direct phone contact to the Facility and Company Security Officers. See <a href="#">Tabs A and C to Appendix 9500</a>	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of facilities.
		<b>A</b> - Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Facility Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		<b>C</b> - Through direct phone contact to the Facility and Company Security Officer.	As soon as possible after obtaining the security information relevant to a class of facilities.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Hand delivery of appropriate security information to the Facility Security Officer and Company Security Officer.	Only when all other means of reaching the facility have failed.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-13
--------------	--------------------	-------------------------------	-----------------------	--------------	-------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3410.4-1: (U) Communication to Commercial Shoreline Facilities (continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Suspicious Activity, Security Breach, and Transportation Security Incident Response Procedures for non-governmental entities to follow (at the unclassified level).	U.S. Coast Guard MSO Jacksonville	<b>P</b> - In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jacksonville Internet. See the 9000 Annex for "green sheet" unclassified procedures.	Not later than 01 July 2004 and updated at least annually.
	JMTX Port Security Committee and Port Canaveral Security Committee	<b>A</b> - Through Port Security Committee educational campaigns aimed at the larger waterway community.	Starting not later than 01 July 2004 and repeated at least annually.
	U.S. Coast Guard MSO Jacksonville	<b>C</b> - Through production of publicly available "greensheet" procedure extracts.	As soon as possible following 01 July 2004.
	MJTF Law Enforcement Ashore and Afloat	<b>E</b> - Delivery of appropriate specific instructions to specific areas, vessels, facilities, and individuals	In extreme emergencies when the SSI incident specific information must be directly provided in order to protect lives, as soon as possible.
Department of Homeland Security Threat Information Bulletins, either at the unclassified level or at the SSI level.	Coast Guard Integrated Command Center	<b>P</b> - Through an unencrypted e-mail or fax to FSOs and CSOs deemed to have a need to know in the opinion of the Federal Maritime Security Coordinator. Where the bulletin is SSI, through an encrypted e-mail in accordance with Section 3590 of this plan. See <u>Tab A and C to Appendix 9500</u> .	As soon as possible after obtaining the DHS Directive
		<b>A</b> - Through fax distribution of a Marine Safety Information Bulletin asking FSOs and CSOs to contact the ICC, sent to entities on the Company and Facility Security Officers.	Within 8 Hours of receiving the DHS Bulletin
		<b>C</b> - Through direct phone contact to the Facility and Company Security Officer.	As soon as possible after obtaining the DHS Bulletin.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Hand delivery of the DHS Bulletin to the Facility Security Officer and Company Security Officer.	Only when all other means of reaching the facility have failed.

See Tab C to Appendix 9500 for detailed points of contact.

Verification of receipt of information from Facilities is required only for communication of specific threats, MARSEC Directives, and MARSEC level changes. The procedures for acknowledging receipt of this information and for verifying attainment of directed security levels and measures can be found in section 3420 and 3430 of this plan.

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS/SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>NE FL SECTOR</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>3000-14</b>
---------------------	----------------------------	---	------------------------------	---------------------	--------------------------	-----------------------------	-------------	----------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



## 3410.5 (U) Communicating with Companies

Communication of security information with Company Security Officers for regulated and non-regulated facilities will be undertaken using prearranged methods that incorporate communication procedures and methods identified in individual facility security plans.

Table 3410.5-1: (U) Communication to Companies. (RESERVED)			
Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Security information relevant to a single company.	Coast Guard Integrated Command Center	<b>P</b> - Through direct phone contact to the Facility/Vessel Security Officer.	As soon as possible after obtaining the security information relevant to a single company.
		<b>A</b> - Through direct phone contact to the Company Security Officer.	As soon as possible after obtaining the security information relevant to a single company.
		<b>C</b> - Through the facility's neighbors and landlords, relaying the message that the FSO is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the ICC cannot make timely contact with the company to communicate the information directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Delivery in person of appropriate security information to the Facility/Vessel Security Officer	Only when all other means of reaching the company have failed.
Security information relevant to an entire class or type of companies (common trade, common ownership, common vessel-callers, etc.), including DHS threat Bullet	Coast Guard Integrated Command Center	<b>P</b> - Through a limited access meeting to distribute Directives - electronic distribution of a notification text page to VSO's and CSO's via email about the meeting. Through direct phone contact to the Vessel and Company Security Officers. See <u>Tab A and C to Appendix 9500</u>	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of facilities.
		<b>A</b> - Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Facility Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		<b>C</b> - Through direct phone contact to the Facility and Company Security Officer.	As soon as possible after obtaining the security information relevant to a class of facilities.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Hand delivery of appropriate security information to the Facility Security Officer and Company Security Officer.	Only when all other means of reaching the facility have failed.
Security information relevant to all companies (regardless of class or type) within a given geographic region or area.	Coast Guard Integrated Command Center	<b>P</b> - Through a limited access meeting to distribute Directives - electronic distribution of a notification text page to CSO's via e-mail about the meeting. Through direct phone contact to the Company Security Officers. See <u>Tab A and C to Appendix 9500</u>	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of facilities.
		<b>A</b> - Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		<b>C</b> - Through direct phone contact to the Facility, Vessel and Company Security Officer.	As soon as possible after obtaining the security information relevant to a class of facilities
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Hand delivery of appropriate security information to the Company Security Officer.	Only when all other means of reaching the company have failed.

See Tab D to Appendix 9500 for detailed points of contact.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-15
--------------	--------------------	-------------------------------	-----------------------	--------------	-------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Verification of receipt of information from Companies is required only for communication of specific threats, MARSEC Directives, and MARSEC level changes. The procedures for acknowledging receipt of this information and for verifying attainment of directed security levels and measures can be found in section 3420 and 3430 of this plan.

## 3410.6 (U) Role of the Port Security Committees

The AMS Committee's role in communicating security information and procedures is pivotal to ensuring that security information can be quickly and effectively transmitted to a broad range of audiences.

33 CFR 103.310 provides that the Port Security Committees' Executive Subcommittees must serve as a link for communicating threats and changes in MARSEC Levels and disseminating appropriate security information to port stakeholders. As such, the Federal Maritime Security Coordinator will convene Executive Subcommittees (separately or in a joint meeting) to advise and assist the FMSC in the communication of security information. The FMSC may convene the Executive subcommittee to seek advice for the following (this list is not meant to be all-inclusive):

- Identify requirements that will need to be implemented from the AMS Plan when notified of an increase in threat;
- Identify requirements that will need to be implemented from the AMS Plan when notified of a MARSEC Directive;
- Communicate threat information through prearranged procedures to MTS/waterway users;
- To convene a lesson learned/hot wash session to develop measurement and improvement strategies after communication portions of the plan have been implemented.

The Executive Subcommittee members must assist the FMSC with the communication requirements identified in this Plan.

## 3420 (U) Security Reporting

The National Response Center (NRC, 1-800-424-8802) will act as the fusion center for all security information required by 33 CFR Part 101, Subpart C, 101.305. The NRC will receive the reports then act as conduit to consequence mitigation and law enforcement organizations. This includes reporting of suspicious activity and actual breaches in security that do not result in a Transportation Security Incident. These reports and the information garnered as a result of follow on investigation will formulate intelligence and threat information that can be used to adjust security conditions throughout the country.

Owners and operators of vessels and facilities with regulatorily -required security plans are required to make reports of suspicious activities, security breaches, and Transportation Security Incidents. Other people are strongly encouraged to make these reports as well using the reporting procedures in this section. Whenever these reports are received by the Coast Guard Integrated Command Center for Northeast and Eastern Central Florida, a Level One activation of the Maritime Joint Task Force (which includes notifications to local authorities) will occur, as outlined in section 5000.

The Federal Maritime Security Coordinator has embarked on a round of discussions through the Maritime Joint Task Force asking that these local authorities, who may receive reports of maritime suspicious activities, security breaches, or even TSIs, make conforming changes to their call receipt procedures and dispatch books such that individuals reporting are reminded to call the National Response Center and to assure the local authorities "close the loop" directly with the Integrated Command Center as well.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-16
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3420.1 (U) Procedures for reporting suspicious activity

Suspicious activities will be reported to the NRC (1-800-424-8802) and the local authorities (911 and 904-247-7318). This section defines the procedures for reporting and responding to a report of suspicious activity occurring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific Suspicious Activities for which the Port Security Committee has developed reporting and response procedures for two general scenarios. These procedures include unclassified guidelines for the port community and Security Sensitive Information procedures for the Maritime Joint Task Force. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The two suspicious activity scenarios include:

- (SA-1) Bomb Threat (UNCLAS Annex)
- (SA-2) Apparent Surveillance, Access Attempt, Suspicious Boating, Suspicious Divers (UNCLAS Annex)

The regulations at 33 CFR part 101.305(a) require the owner and operator of vessels and facilities with regulatorily-required security plans to report suspicious activities, and specific procedures meeting these regulatory requirements are contained in the above two suspicious activity annexes. Other vessels and facilities are hereby encouraged, but not required, to report suspicious activities as well. To fully implement this policy of encouraging non-regulated entities to report suspicious activities, the FMSC routinely re-emphasizes the policy through a variety of public communication means including Marine Safety and Security Information Bulletins, press releases, discussions with the Port Security Committee general membership, and re-emphasis during visits and patrols, particularly including marina visits.

## 3420.2 (U) Procedure for Reporting Breaches in Security

This section defines the procedures for reporting and response to a breach of security occurring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific breaches of security for which the Port Security Committee has developed reporting and response procedures for four general scenarios. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The four security breach scenarios include:

- (SB-1) Trespass Ashore, Stowaway Discovered, or Smallboat in Security Zone (UNCLAS Annex)
- (SB-2) Small-scale illegal demonstration (UNCLAS Annex)
- (SB-3) Evidence of Tampering w/ Security Systems (UNCLAS Annex)
- (SB-4) Security Measures Not in Place (UNCLAS Annex)

The regulations at 33 CFR part 101.305(b) require the owner and operator of vessels and facilities with regulatorily-required security plans to report security breaches, and specific procedures meeting these regulatory requirements are contained in the above four security breach annexes. Other vessels and facilities are hereby encouraged, but not required, to report security breaches as well. To fully implement this policy of encouraging non-regulated entities to report security breaches, the FMSC routinely re-emphasizes the policy through a variety of public communication means including Marine Safety and Security Information Bulletins, press releases, discussions with the Port Security Committee general membership, and re-emphasis during visits and patrols, particularly including marina visits.

VERSION DATE	V.1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-17
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3420.3 (U) Procedure for Reporting Transportation Security Incidents (TSIs)

A TSI should be first be reported to the appropriate emergency services (dial 911) to ensure human health and safety measures are taken. Secondary notifications should be made to the Coast Guard Federal Maritime Security Coordinator (dial 904-247-7318 for the Coast Guard Integrated Command Center), then to the National Response Center (dial 1-800-424-8802). This section defines the procedures for reporting and responding to a transportation security incident occurring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific TSIs for which the Port Security Committee has developed reporting and response procedures for eleven specific scenarios. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The eleven TSI scenarios include:

- (TSI1) Possible or Actual Rogue Vessel (UNCLAS Annex)
- (TSI2) Outbreak of Disease on Vessel (UNCLAS Annex)
- (TSI3) Explosive Device Discovery (UNCLAS Annex)
- (TSI4) Intrusion Ashore w/ small arms (UNCLAS Annex)
- (TSI5) Suspect Cargo including WMD (UNCLAS Annex)
- (TSI6) Suspect Crewmen or Employee (UNCLAS Annex)
- (TSI7) Small Boat Attack (UNCLAS Annex)
- (TSI8) Report of Gunfire in the Port (UNCLAS Annex)
- (TSI9) Explosion (cause unknown), ship or port (UNCLAS Annex)
- (TSI10) Mass Illegal Demonstration (UNCLAS Annex)
- (TSI11) Evacuation of a section of the port (UNCLAS Annex)

## 3430 (U) Communicating MARSEC Directives

As provided for in Title 33 CFR part 101.405, the Coast Guard may issue MARSEC Directives to provide vessels and facilities nationwide with objective performance standards regarding access control and the secure handling of cargo. These directives will play a vital role in the successful implementation of the MTSA regulations in many ways.

MARSEC Directives allow the Commandant to ensure that there is consistency throughout the country when enforcing the provisions of the MTSA by providing COTPs objective standards by which the performance of vessels and facilities nationwide will be evaluated.

MARSEC Directives allow the Coast Guard the flexibility to tailor objective performance standards to the prevailing threat environment or industry segment. For example, if high capacity ferry vessels are at a greater risk for a TSI, the Coast Guard may issue a directive that would require enhanced security measures typical of a higher MARSEC Level that would apply only to that segment of the maritime industry.

MARSEC Directives will not impose new requirements, but provide direction to the industry on how to meet the performance standards already required by the regulations. The regulations further provide that the directives will only be issued by Commandant, and only after consultation with other interested Federal agencies within the Department of Homeland Security.

VERSION DATE	V.1.1 26 MAY 04	CLASSIFICATION:	UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-18
-----------------	--------------------	-----------------	------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3430.1 (U) Procedures for Communicating Security Directives

When a new MARSEC Directive is issued, the Coast Guard will publish a notice in the Federal Register and announce through other means (i.e. text page/e-mail notification) that it has issued a new MARSEC Directive. The MARSEC Directives will be individually numbered, and will be assigned to a series that corresponds with the part of this subchapter to which the MARSEC Directive refers. For example, the first MARSEC Directive addressing a new requirement for vessels regulated under part 104 of this subchapter would be identified as MARSEC Directive 104-01.

Upon receiving notice that a new MARSEC Directive has been issued, affected entities must contact the local COTP ( if appropriate, their District Commander) to receive a copy of the MARSEC Directive. The COTP or District Commander will confirm, prior to distributing the MARSEC Directive, that the requesting entity is a “covered person” or a person with a “need to know”, and that the requesting entity will safeguard the MARSEC Directive as SSI.

Thus, continuing with the example of the previous paragraph, upon receiving notice that a MARSEC Directive in the 104 series has been issued, owners and operators of vessels covered by part 104 of this subchapter need to contact their local COTP to obtain a copy of the MARSEC Directive. They would then be required to comply with the MARSEC Directive, or follow the procedures set out in the MARSEC Directive for gaining approval of an equivalent security measure.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-19
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3430.1-1: (U) Dissemination of MARSEC Directives**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
An alert that new MARSEC Directives have been published (indicating that port entities need to find out whether they apply or not)	Commandant	<b>P</b> – Published notice in the Federal Register (available online at: [web address])	Within 24 hours of issuing the MARSEC Directive.
	Port Security Committee Co-chairs	<b>A</b> – Text Page/E-mail MSIB to mass distribution (all VSOs, CSOs, and FSOs) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives.	Within 24 hours of Commandant issuing the MARSEC Directive.
	FMSC	<b>C</b> – Fax distribution MSIB to port entities (all VSOs, CSOs, and FSOs) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives.	Within 72 hours of Commandant issuing the MARSEC Directive.
	FMSC	<b>E</b> – Phone call to emergency 24-hour contact number informing CSOs, VSOs, and FSOs that the MARSEC Directives have been issued.	Only when specific entities do not come forward to collect a Directive or when the situation is urgent.
The date, time and location of a mass-distribution meeting for a new MARSEC Directive.	FMSC	<b>P</b> – Text Page/E-mail MSIB to mass distribution (all VSOs, CSOs, and FSOs) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives. May be combined with the alert that the directives were issued.	Within 24 hours of Commandant issuing the MARSEC Directive.
	FMSC	<b>A</b> – Fax distribution MSIB to port entities (all VSOs, CSOs, and FSOs) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives.	Within 72 hours of Commandant issuing the MARSEC Directive.
	Port Security Committees	<b>C</b> – Phone-tree notification by select SSI-capable members of the Port Security Committee to fellow all VSOs, CSOs, and FSOs.	Within 72 hours of Commandant issuing the MARSEC Directive.
	FMSC	<b>E</b> – Phone call to emergency 24-hour contact number informing CSOs, VSOs, and FSOs where and when the MARSEC Directives will be distributed.	Only when the Directive is an emergency.
The applicability of a specific new MARSEC Directive to a specific Company or Facility.	FMSC	<b>P</b> – Via discussion at the Distribution meeting.	Within 72 hours of Commandant issuing the MARSEC Directive.
		<b>A</b> – Via phone discussion with the VSO/FSO.	Only when the Directive is an emergency.
		<b>C</b> – Via e-mail to the VSO/FSO	Only when the Directive is an emergency.
		<b>E</b> – Via in-person discussion following hand delivery of the MARSEC Directive	Only when the Directive is an emergency.

<b>VERSION DATE</b>	<u>V_1.1</u> 26 MAY 04	<b>CLASSIFICATION:</b> UNCLAS/SSI	<b>CONTROLLING AUTHORITY</b>	NE FL SECTOR	<b>ISSUING AUTHORITY</b>	<u>CAPT</u> D.L. LERSCH	<b>PAGE</b>	3000-20
---------------------	---------------------------	--------------------------------------	------------------------------	--------------	--------------------------	----------------------------	-------------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



**Table 3430.1-1: (U) Dissemination of MARSEC Directives (continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
The MARSEC Directive itself.	FMSC	P - Via personal "need to know" verification, Identity verification, and SSI Agreement signature at the Distribution meeting.	Within 72 hours of Commandant issuing the MARSEC Directive.
		A - Via encrypted e-mail following phone "need to know" verification, Identity verification, and SSI Agreement signature receipt.	Only when the Directive is an emergency.
		C - Via fax following phone "need to know" verification, Identity verification, and SSI Agreement signature receipt.	Only when the Directive is an emergency.
		E- Via in-person discussion following hand delivery of the MARSEC Directive	Only when the Directive is an emergency.

The Federal Maritime Security Coordinator keeps track of each and every MARSEC Directive communication as required for dissemination of any Sensitive Security Information document. Specifically, the information is recorded in two fashions: first, a paper log book containing the date, time, location, type of SSI (in this case a MARSEC Directive), person receiving, person distributing, and confirmation of covered-person and need-to-know determination is completed at the time of dissemination. Second, the same information is recorded in a centralized SSI-distribution tracking database which can be sorted according to person receiving, date, document distributed, or other criteria. These records are maintained in accordance with Coast Guard Commandant Instruction 5510.5.

## 3430.2 (U) Procedures for Responding to MARSEC Directives

Once a MARSEC Directive has been issued it is the responsibility of the affected entities to confirm compliance with the Directive, to the local COTP and specify the method by which the mandatory measures in the directive has been, or will be, met. In some cases recipients may elect to submit proposed equivalent security measures to the local COTP if the recipient is unable to implement the measures mandated in the MARSEC Directive. However, the entity will only be able to propose such alternatives for the length of time specified in the MARSEC Directive, and he/she will be required to implement any alternative measures that the COTP does approve.

**Table 3430.2-1: (U) Responding to MARSEC Directives**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Vessel, facility, or other port entity has received and acknowledges receiving a MARSEC Directive	VSO, FSO, and/or CSO	<b>P</b> - Signing the SSI / MARSEC Directive sign-out sheet at the FMSC's distribution meeting	Within 72 hours of Commandant issuing the MARSEC Directive.
		<b>A</b> - Submitting the web-page MARSEC Directive Acknowledged message to the Coast Guard ICC.	Immediately upon receiving the MARSEC Directive where signing the SSI/MARSEC Directive sign-out sheet is not possible.
		<b>C</b> - Submitting a personal letter acknowledgement via fax to the Coast Guard ICC	Immediately upon receiving the MARSEC Directive where signing the SSI/MARSEC Directive sign-out sheet is not possible.
		<b>E</b> - Submitting a personal letter in person to the Coast Guard Marine Safety Office at 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211.	As soon as possible after receiving the MARSEC Directive where signing the SSI/MARSEC Directive sign-out sheet is not possible.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-21
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3430.2-1: (U) Responding to MARSEC Directives (continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Vessel, facility, or other port entity has complied with the requirements of a MARSEC Directive.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Directive Attainment message to the Coast Guard ICC.	Immediately upon complying fully with the MARSEC Directive.
		<b>A</b> - Submitting a personal letter attainment report via fax to the Coast Guard ICC	Immediately upon complying fully with the MARSEC Directive.
		<b>C</b> - Submitting a personal letter in person to the Coast Guard Marine Safety Office at 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211.	Immediately upon complying fully with the MARSEC Directive.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center.	Immediately upon complying fully with the MARSEC Directive – emergency situations only.
Vessel, facility, or other port entity has received a MARSEC Directive but cannot implement the requirements of the Directive until questions are answered.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Directive Questions message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>A</b> - Submitting a personal letter asking questions via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon complying fully with the MARSEC Directive – emergency situations only.
Vessel, facility, or other port entity has received a MARSEC Directive but cannot implement the requirements of the Directive at all.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Directive SHORTFALL message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>A</b> - Submitting a personal letter noting the SHORTFALL via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon complying fully with the MARSEC Directive – emergency situations only.
Vessel, facility, or other port entity has received a MARSEC Directive but requests permission from the Federal Maritime Security Coordinator to implement an alternative measure accomplishing the Directive's objective.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Directive ALTERNATIVE REQUEST message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>A</b> - Submitting a personal letter noting the ALTERNATIVE REQUEST via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon complying fully with the MARSEC Directive – emergency situations only.
Vessel, facility, or other port entity has received a MARSEC Directive but requests an extension for additional time to implement the specific requirements of the Directive fully.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Directive EXTENSION REQUEST message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>A</b> - Submitting a personal letter noting the EXTENSION REQUEST via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the MARSEC Directive.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon complying fully with the MARSEC Directive – emergency situations only.

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS/SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>NE FL SECTOR</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>3000-22</b>
---------------------	----------------------------	---	------------------------------	---------------------	--------------------------	-----------------------------	-------------	----------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

WEB PAGE [http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication\\_email.htm](http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication_email.htm)

The Federal Maritime Security Coordinator and the Maritime Joint Task Force will conduct law enforcement and inspection activities to verify that recipients of MARSEC Directives, once they report attaining the directed measures, are in fact implementing them.

Waiver requests and Captain of the Port permission to implement approved equivalent measures will be dealt with by the Captain of the Port by priority and in writing. Entities which have submitted these waivers and equivalency requests are required to comply with the MARSEC Directive requirements unless the Captain of the Port communicates by phone interim approval while the formal request is under review. All such phone interim approvals will immediately be followed by written documentation of same transmitted by fax to the affected Vessel Security Officer, Facility Security Officer, or Company Security Officer.

### 3430.3 (U) Role of the Port Security Committees

33 CFR 103.310 directs the Port Security Committee Executive Subcommittees to serve as a link for communicating threats and changes in MARSEC levels and disseminating appropriate security information to port stakeholders. Accordingly, the FMSC may from time to time and to different degrees require the Executive Subcommittee to assist in the distribution of MARSEC Directives.

Until such time as the Executive Subcommittees can develop procedures and protocols addressing how they will contribute on a routine basis to this effort, the Executive Subcommittee will assist only as specifically requested by the FMSC and using the procedures and protocols directed by the FMSC.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-23
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3440 (U) Communicating MARSEC Levels

MARSEC levels will be set commensurate with the Homeland Security Advisory System (HSAS). The Secretary of Homeland Security sets the HSAS threat condition and only the Commandant will have the authority to change MARSEC levels to match the HSAS. See section 4000 for a more detailed discussion of the link between HSAS and MARSEC levels.

An exception to this rule is provided for the FMSCs to temporarily raise the MARSEC level in his/her zone to address an immediate threat to the MTS when the immediacy of the threat or incident does not allow time to notify the Commandant. The FMSC will only exercise this authority in the most immediate and urgent circumstances. Such circumstances would include immediate action to save lives, mitigate great property damage or environmental damage resulting from a TSI and timely prior notification to the Commandant is not possible. If such a circumstance does arise the FMSC must immediately inform the Commandant via the chain of command. The heightened MARSEC level will only continue as long as necessary to address the serious threat which prompted the setting of the raised level.

### 3440.1 (U) Procedures to Communicate Changes in MARSEC Levels

Table 3440.1-1(U) Communicating Changes in MARSEC Levels

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Change in MARSEC	Coast Guard Integrated Command Center	<b>P</b> - Through text page and electronic distribution of a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
		<b>A</b> - Through fax distribution of the same Marine Safety Information Bulletin to entities on the volunteer subscription list and all VSOs, CSOs, and FSOs.	Within 8 Hours of MARSEC level changes and associated waterway closures.
		<b>C</b> - Recurring Broadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	<b>E</b> - Posting of notices in marinas, yacht clubs, tackle and bait stores, and marine supply shops.	Only when electronic, fax and radio distribution systems are not functional and/or deemed inadequate due to insufficient subscription.
Threat Intel causing MARSEC change	RESERVED	RESERVED	RESERVED
Security Measures in AMSP	RESERVED	RESERVED	RESERVED

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-24
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 3440.2 (U) Reporting Attainment of MARSEC Levels

33 CFR Part 104, 105, and 106 require that regulated entities report that they have received notification of changes in MARSEC level and that they have implemented the appropriate measures in accordance with their plan. This will place a great deal of burden on the communication systems in the port.

**Table 3440.2-1: (U) Reporting Attainment of MARSEC Level**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Vessel, facility, or other port entity has received and acknowledges receiving a MARSEC level change	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC level change Acknowledged message to the Coast Guard ICC.	Immediately upon receiving the MARSEC Level Change information.
		<b>A</b> – Submitting a personal letter acknowledgement via fax to the Coast Guard ICC	Immediately upon receiving the MARSEC Level Change information.
		<b>C</b> – Making a level-change acknowledgement phone call to the Coast Guard ICC at (904) 247-7318.	Immediately upon receiving the MARSEC Level Change information.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center.	Emergencies when all other means have failed.
Vessel, facility, or other port entity has complied with the requirements of a MARSEC Level Change as outlined in the Facility Security Plan, Vessel Security Plan, and Area Maritime Security Plan.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Directive Attainment message to the Coast Guard ICC.	Immediately upon fully instituting all Security measures for the new MARSEC Level (up or down).
		<b>A</b> – Submitting a personal letter attainment report via fax to the Coast Guard ICC	Immediately upon fully instituting all Security measures for the new MARSEC Level (up or down).
		<b>C</b> – Making a level-change acknowledgement phone call to the Coast Guard ICC at (904) 247-7318.	Immediately upon fully instituting all Security measures for the new MARSEC Level (up or down).
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center.	Emergencies when all other means have failed.
Vessel, facility, or other port entity has received a MARSEC level change but cannot implement the requirements of the Directive until questions are answered.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Level Change Questions message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the MARSEC Level Change.
		<b>A</b> – Submitting a personal letter asking questions via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the MARSEC Level Change.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the MARSEC Level Change.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon complying fully with the MARSEC Level Change – emergency situations only.
Vessel, facility, or other port entity has received a MARSEC Level Change but cannot implement the all or some of the Security Measures identified in the Facility Security Plan, Vessel Security Plan, or Area Maritime Security Plan for the new MARSEC level.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC LEVEL SHORTFALL message to the Coast Guard ICC.	Immediately upon identifying Security measures for the new MARSEC Level which cannot be instituted.
		<b>A</b> – Submitting a personal letter noting the SHORTFALL via fax to the Coast Guard ICC	Immediately upon identifying Security measures for the new MARSEC Level which cannot be instituted.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon identifying Security measures for the new MARSEC Level which cannot be instituted.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon identifying Security measures for the new MARSEC Level which cannot be instituted – emergency situations only.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-25
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Table 3440.2-1: (U) Reporting Attainment of MARSEC Level (continued)**

<u>Information to Communicate</u>	<u>Who communicates</u>	<u>How the Information Is Communicated</u>	<u>When the Information Is Communicated</u>
Vessel, facility, or other port entity has received a MARSEC Level Change but requests permission from the Federal Maritime Security Coordinator to implement an alternative measure than those outlined in the Facility Security Plan, Vessel Security Plan, or Area Maritime Security Plan accomplishing the MARSEC Level's objective.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Level ALTERNATIVE REQUEST message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level.
		<b>A</b> - Submitting a personal letter noting the ALTERNATIVE REQUEST via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level – emergency situations only.
Vessel, facility, or other port entity has received a MARSEC Level Change but requests an extension for additional time to implement the specific Security Measures in the Facility Security Plan, Vessel Security Plan, or Area Maritime Security Plan fully.	VSO, FSO, and/or CSO	<b>P</b> – Submitting the web-page MARSEC Level EXTENSION REQUEST message to the Coast Guard ICC.	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level.
		<b>A</b> - Submitting a personal letter noting the EXTENSION REQUEST via fax to the Coast Guard ICC	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level.
		<b>C</b> – Calling the Coast Guard Integrated Command Center at (904) 247-7318.	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level.
		<b>E</b> – Via Radio VHF Channel 16 to the Coast Guard Integrated Command Center, to establish land-line non-emergency means of discussion.	Immediately upon receiving and attempting to comply fully with the Security measures outlined for the new MARSEC level – emergency situations only.

The Federal Maritime Security Coordinator and the Maritime Joint Task Force will conduct law enforcement and inspection activities to verify vessels, facilities, and other entities, once they report attaining higher security levels, are in fact implementing security measures specified in their plans and in this Area Maritime Security Plan. Entities that cannot or do not attain the required security levels are considered a security breach under 33 CFR part 101, and as such the Federal Maritime Security Coordinator may take emergency governmental action with the Maritime Joint Task Force to re-establish the necessary level of security, may direct the owner and operator to implement specific emergency security measures to reestablish the necessary level of security, and may additionally take such administrative, civil, and criminal law enforcement action as is necessary to remedy the situation and deter future breaches of security.

Waiver requests and Captain of the Port permission to implement approved equivalent measures will be dealt with by the Captain of the Port by priority and in writing. Entities which have submitted these waivers and equivalency requests are required to comply with their security plans and this AMS Plan unless the Captain of the Port communicates by phone interim approval while the formal request is under review. All such phone interim approvals will immediately be followed by written documentation of same transmitted by fax to the affected Vessel Security Officer, Facility Security Officer, or Company Security Officer.

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS/SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>NE FL SECTOR</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>3000-26</b>
---------------------	----------------------------	---	------------------------------	---------------------	--------------------------	-----------------------------	-------------	----------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



## 3440.3 (U) Role of Area Maritime Security (AMS) Committee

33 CFR 103.310 directs the Port Security Committee Executive Subcommittees to serve as a link for communicating threats and changes in MARSEC levels and disseminating appropriate security information to port stakeholders. Accordingly, the FMSC may from time to time and to different degrees require the Executive Subcommittee to assist in the communication of changes in MARSEC level.

Until such time as the Executive Subcommittees can develop procedures and protocols addressing how they will contribute on a routine basis to this effort, the Executive Subcommittee will assist only as specifically requested by the FMSC and using the procedures and protocols directed by the FMSC.

## 3500 (U) Security Sensitive Information

This section governs the designation of information, personnel, maintenance, safeguarding, and disclosure of records and information that has been determined to be Sensitive Security Information (SSI) as defined in para. 3510. This section does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is exempt from public disclosure under the Freedom of Information Act. This section is organized as follows:

- 3510 Information Constituting Security Sensitive Information
- 3520 Covered Persons
  - 3520.1 Designation as a Covered Person
- 3530 Restrictions on the Disclosure of SSI
- 3540 Persons with a Need to Know
- 3550 Marking of SSI
- 3560 Disclosure by TSA and Coast Guard
- 3570 Consequences of Unauthorized SSI Disclosure
- 3580 Destruction of SSI
- 3590 Procedures for Communicating SSI Material

## 3510 (U) Information Constituting Security Sensitive Information

**General.** In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which has been determined would—

- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
- (2) Reveal trade secrets or privileged or confidential information obtained from any person; or
- (3) Be detrimental to the security of transportation.

**Information constituting SSI.** Except as otherwise provided in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-27
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- (1) **Security programs and contingency plans.** Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including—
  - (i) Any vessel, maritime facility, or port area security plan required or directed under Federal law;
  - (ii) Any national or area security plan prepared under 46 U.S.C. 70103; and
  - (iii) Any security incident response plan established under 46 U.S.C. 70104.
- (2) **Security Directives.** Any Security Directive or order—
  - (i) Issued by TSA under § 1542.303, § 1544.305, or other authority;
  - (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or
  - (iii) Any comments, instructions, and implementing guidance pertaining thereto.
- (3) **Information Circulars.** Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—
  - (i) Information Circular issued by TSA under § 1542.303, § 1544.305, or other authority; and
  - (ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.
- (4) **Performance specifications.** Any performance specification and any description of a test object or test procedure, for—
  - (i) Any device used by the Federal government or any other person pursuant to any maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and
  - (ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any maritime transportation security requirements of Federal law.
- (5) **Vulnerability assessments.** Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.
- (6) **Security inspection or investigative information.** Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.
- (7) **Threat information.** Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.
- (8) **Security measures.** Specific details of maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—
  - (i) Security measures or protocols recommended by the Federal government;
  - (ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties, to the extent it is not classified national security information.
- (9) **Security screening information.** The following information regarding security screening under maritime transportation security requirements of Federal law:

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-28
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- (i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.
  - (ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.
  - (iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by the COTP to be SSI.
  - (iv) Any security screener test and scores of such tests.
  - (v) Performance or testing data from security equipment or screening systems.
  - (vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.
- (10) **Security training materials.** Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any maritime transportation security measures required or recommended by DHS or DOT.
- (11) **Identifying information of certain transportation security personnel.** Lists of the names or other identifying information that identify persons as —
- (i) Having unescorted access to a secure area or restricted area of a maritime facility, port area, or vessel or;
  - (ii) Holding a position as a security screener employed by or under contract with the Federal government pursuant to maritime transportation security requirements of Federal law.
  - (iii) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;
- (12) **Critical maritime infrastructure asset information.** Any list identifying systems or assets, whether physical or virtual, so vital to the maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is —
- (i) Prepared by DHS or DOT; or
  - (ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.
- (13) **Systems security information.** Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.
- (14) **Confidential business information.**
- (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising thereof, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to maritime transportation security measures;
  - (ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out maritime transportation security responsibilities; and
  - (iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out maritime transportation security responsibilities, but only if the source of the information does

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-29
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

not customarily disclose it to the public.

- (15) **Research and development.** Information obtained or developed in the conduct of research related to maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.
- (16) **Other information.** Any information not otherwise described in this section that the DHS determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the DHS or the Secretary of DOT may designate as SSI information not otherwise described in this section.

## 3520 (U) Covered Persons

Covered person means any organization, entity, individual, or other person described in para. 3520.1. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in 3520.1

### 3520.1(U) Designation as a Covered Person.

The following are designated as Covered Persons:

- (a) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.
- (b) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR part 6, or 33 U.S.C. 1221 et seq.
- (c) Each person performing the function of a computer reservation system or global distribution system for cruise line passenger information.
- (d) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.
- (e) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.
- (f) DHS and DOT.
- (g) Each person conducting research and development activities that relate to maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.
- (j) Each person who has access to SSI, as specified in para. 3540.
- (k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-30
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- (l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.
- (k) Each person receiving SSI under paragraph 3540.

## 3530 (U) Restrictions on the Disclosure of SSI.

**Duty to protect information.** A covered person must—

- (1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.
- (2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by the Commandant of the Coast Guard, or the Secretary of DOT.
- (3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.
- (4) Mark SSI as specified in para. 3550.
- (5) Dispose of SSI as specified in para. 3570.

**Unmarked SSI.** If a covered person receives a record containing SSI that is not marked as specified in para. 3530, the covered person must—

- (1) Mark the record as specified in para. 3550 and
- (2) Inform the sender of the record that the record must be marked as specified in para. 3550.

**Duty to report unauthorized disclosure.** When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

## 3540 (U) Persons with a Need to Know

**General.** A person has a need to know SSI in each of the following circumstances:

- (1) When the person requires access to specific SSI to carry out maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.
- (2) When the person is in training to carry out maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.
- (3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out maritime transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.
- (4) When the person needs the information to provide technical or legal advice to a covered person regarding maritime transportation security requirements of Federal law.
- (5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding, except that in the case of an individual serving as litigation counsel who is not a direct employee of the covered person—
  - (i) The individual has a need to know only if, in the judgment and sole discretion of the DHS or the Secretary of DOT, access to the SSI is necessary for the litigation counsel to represent the covered person in the proceeding; and

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-31
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

(ii) The DHS or the Secretary of DOT may make the individual's access to the SSI contingent upon satisfactory completion of a security background check and the imposition of a protective order or agreed upon procedures that establish requirements for safeguarding SSI that are satisfactory to the Administrator or the Secretary of DOT.

**Federal employees, contractors, and grantees.**

A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties. A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary for performance of the contract or grant.

**Need to know further limited by the DHS or DOT.** For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

## 3550 (U) Marking SSI.

**Marking of paper records.** In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

- (1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;
- (2) Any title page; and
- (3) Each page of the document.

**Protective marking.** The protective marking is: SENSITIVE SECURITY INFORMATION.

**Distribution limitation statement.** The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

**Other types of records.** In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

## 3560 (U) SSI disclosed By TSA or the Coast Guard

**General.** Except as provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does the Department of Homeland Security release such records to persons without a need to know.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-32
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



**Disclosure under the Freedom of Information Act and the Privacy Act.** If a record contains both SSI and information that is not SSI, TSA or the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

**Disclosures to committees of Congress and the General Accounting Office.** Nothing in this part precludes TSA or the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

#### **Disclosure in enforcement proceedings.**

**General.** TSA or the Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the DHS or the Commandant of the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by TSA or the Coast Guard.

**Security background check.** Prior to providing SSI to a person under paragraph (d)(1) of this section, TSA or the Coast Guard may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the DHS or the Commandant of the Coast Guard, a security background check.

**Obligation to protect information.** When an individual receives SSI, that individual becomes a covered person under para. 3520.1 and is subject to the obligations of a covered person under this part.

**No release under FOIA.** When TSA discloses SSI pursuant to this paragraph, TSA makes the disclosure for the sole purpose of providing the information to a person for preparation of a response to allegations contained in a legal enforcement action document. Such disclosure is not a public release of information under the Freedom of Information Act.

**Disclosure in the interest of safety or security.** The Department of Homeland Security, the Commandant of the Coast Guard, or the Secretary of the Department of Transportation may disclose SSI where necessary in the interest of public safety or in furtherance of transportation security.

## **3570 (U) Consequences of Unauthorized SSI Disclosure**

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by the Department of Homeland Security, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

## **3580 (U) Destruction of SSI.**

**Department of Homeland Security.** Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-33
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

**Other covered persons.** A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

**Exception.** This section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

## 3590 (U) Procedures for communicating SSI material.

**General.** SSI material is to be disseminated to Port Security Committee members and/or port stakeholders in accordance with U.S. Coast Guard Commandant Instruction 5510.5. This instruction, in its entirety, has been designated SSI.

**Hard Copy Dissemination.** Hard copy dissemination may be accomplished via U.S. Mail, interoffice mail, hand carrying within/between buildings; with strict packaging and delivery mandates to ensure privacy.

**Electronic Transmission.** Electronic transmission of SSI may be accomplished via:

**Facsimile.** The sender must confirm that the facsimile number of the recipient is current and valid and the facsimile machine is in a controlled area where unauthorized persons cannot intercept the SSI facsimile; or the sender must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information. The information to be transmitted must have a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that, if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

**Electronic Mail.** SSI must be transmitted in a password protected attachment.

**Telephone.** The caller must ensure that the person receiving the SSI is an authorized recipient. Individuals needing to pass SSI by telephone shall avoid using cellular telephones and cordless telephones unless the circumstances are exigent, or the transmissions are encoded or otherwise protected to reduce the risk of interception and monitoring.

**Wireless devices.** Do not use cellular phones, pagers, cordless telephones, personal digital assistants to transmit SSI. The risk of interception and monitoring is greater when using wireless devices unless there is an emergency or the transmissions are encrypted.

**Internet.** Internet posting of SSI is allowed if within a secure socket layer (SSL) with minimum access controls consisting of a user name, password and Primary Content Approval Officials (PCAOs) ensuring that no documents/databases containing SSI information are released. In addition to the SSL and PCAOs, FMSCs may also include SSI warning banners upon logon; Electronically signed non-disclosure agreements at each logon; Limited user permissions (based on need-to-know); and Limitations on storage of SSI information.

## 3600 (U) Maritime Security Training

Each member of the Port Security Committee is responsible for ensuring those members of their organization directly affected by the execution of the AMS Plan are trained to an appropriate level to execute their roles in implementing the AMS Plan. The Coast Guard will not be involved in any maritime security training of commercial personnel. However, we can provide a list of maritime security training topics/courses that every person should be familiar with or had some type of training on. In addition, below are several links that will prove beneficial to your training needs.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-34
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Hazardous Material I, II, III  
Incident Command System (ICS) 100, 200, 300, 400 Level  
Explosive & Weapons of Mass Destruction (WMD)

[FEMA Education & Training](#)  
[Florida Emergency Management \(Training & Event schedule\)](#)  
[Florida Emergency Management on Terrorism](#)  
[Florida State Emergency Response Commission](#)  
[Incident Command System](#)

## 3700 (SSI) Security Resources

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS/SSI	CONTROLLING AUTHORITY	NE FL SECTOR	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	3000-35
-----------------	--------------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4000 ANNEX – PREVENTION

- 4100 INTRODUCTION
- 4200 MARITIME SECURITY MARSEC LEVEL PLANNING
  - 4210 Link to Homeland Security Advisory System
  - 4220 Procedures when vessel & facility are at different MARSEC
  - 4230 Procedures for requesting equivalencies to MARSEC Directives
- 4300 MARSEC LEVEL 1
  - 4310 Roles, Resources, Authorities, and Responsibilities
  - 4320 Standard Security Procedures for MARSEC Level 1
  - 4330 Physical Security Measures
  - 4340 Operational Security (OPSEC) Measures
  - 4350 Security Measures for Sea Port of Embarkation Operations
- 4400 MARSEC LEVEL 2
  - 4410 Roles, Resources, Authorities, and Responsibilities
  - 4420 Standard Security Procedures for MARSEC Level 2
  - 4430 Physical Security Measures
  - 4440 Operational Security Measures
  - 4450 Security Measures for Sea Port of Embarkation Operations
- 4500 MARSEC LEVEL 3
  - 4510 Roles, Resources, Authorities, and Responsibilities
  - 4520 Standard Security procedures for MARSEC Level 3
  - 4530 Physical Security Measures
  - 4540 Operational Security Measures
  - 4550 Security Measures for Sea Port of Embarkation Operations
- 4600 PUBLIC ACCESS FACILITY
  - 4610 Designation of Public Access Facilities
  - 4620 Withdrawal of Designation
  - 4630 Security Procedures for Public Access Facilities
- 4700 MARITIME WORKER CREDENTIALS

### 4100 (U) Introduction

MARSEC Levels were established to allow the Coast Guard to easily and clearly communicate the security measures required in response to an HSAS Threat Condition. MARSEC Levels permit FMSCs, in consultation with the Port Security Committee, to plan and pre-designate appropriate preventative and protective postures for each MARSEC Level. The three MARSEC Levels align with the five color-coded HSAS Threat Conditions. Because of the unique nature of the maritime industry, MARSEC Level 1 applies when HSAS Threat Conditions Green, Blue, and Yellow are set. MARSEC Level 2 corresponds to HSAS Threat Condition Orange, while MARSEC Level 3 corresponds to HSAS Threat Condition Red.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION:	UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-1
-----------------	--------------------	-----------------	--------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4200 (U) Maritime Security (MARSEC) Level Planning

This section is organized as follows:

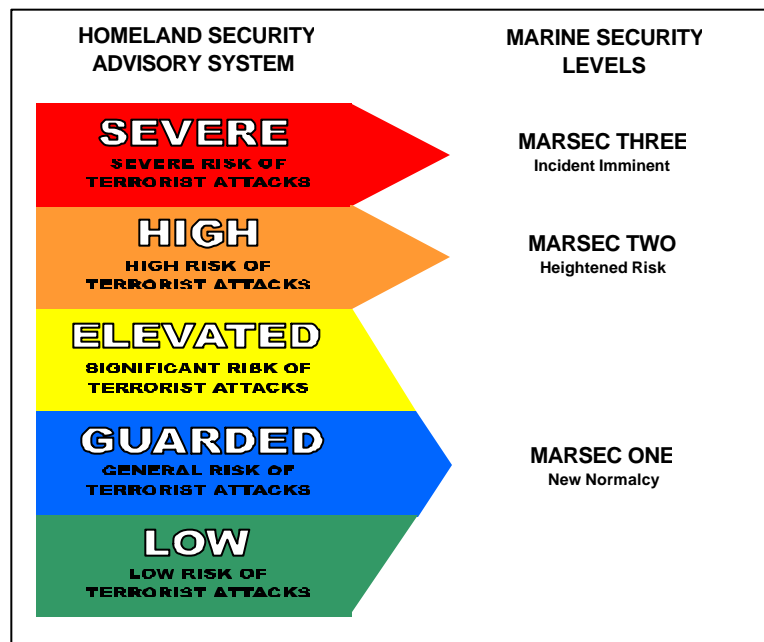
- 4210 [Link to Homeland Security Advisory System](#)
- 4220 [Procedures when a Vessel and Facility are at Different](#)
- 4230 [Procedures for Requesting Equivalencies to MARSEC Directives](#)

### 4210 (U) Link to Homeland Security Advisory System

Given that the Secretary of the Department of Homeland Security manages HSAS Threat Conditions as a national system, only the Commandant of the Coast Guard can set MARSEC Levels, and MARSEC changes will occur when the threat that prompted a change in the HSAS Threat Condition imperils the Marine Transportation System (MTS).

There may be instances where DHS raises the HSAS Threat Condition based on threats unrelated to the MTS, the threat becomes more defined and it is clear that the MTS is not a target. In these instances, the Commandant may set MARSEC Levels below the equivalent HSAS Threat Condition. Furthermore, it may be appropriate for the Commandant to raise the MARSEC Level at only specific ports in response to the elevated HSAS Threat Condition instead of requiring all ports nationwide or on a particular coast to elevate their protective measures. Examples include ports where military load-outs occur or those considered strategically important.

FMSCs may temporarily raise the MARSEC Level in their respective AOR or for a segment of the maritime industry within that area only when there is a serious threat to the MTS requiring immediate action to prevent a TSI and timely consultation with the Commandant is not feasible. The heightened MARSEC Level will continue only as long as necessary to address the serious threat which prompted the FMSC to set that Level. An example would be a situation in which the FMSC receives information from the local police that a bomb has been located at a Liquefied Natural Gas (LNG) facility while a LNG ship is inbound to the facility. It is anticipated that COTPs would raise the MARSEC Level only in the most rare of circumstances.



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-2
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4220 (U) Procedures when Vessel and Facility are at different MARSEC Levels

There may be circumstances (i.e. directed by their flag state or at the discretion of the vessel owner) where a vessel is operating at a higher maritime Security Level, as defined by the ISPS Code, than the port that the vessel is calling on. In such cases, the port and its facilities may remain at the existing MARSEC Level. However, if the port or facility is at higher MARSEC Level per Commandant or the FMSC's direction than the arriving vessel, the foreign flagged vessel must attain the corresponding MARSEC Level. The assumption is made that U.S. flagged vessels will already be at a corresponding MARSEC level with the receiving facility but the ship's agent is still responsible for prior notification of the facility's and vessel's MARSEC Levels.

The responsibility to notify adjacent facilities within 500 meters of the receiving facility of the higher MARSEC Level of the arriving ship remains with the receiving facility. The arriving foreign flagged vessel that is at a higher maritime Security Level must complete a Declaration of Security (regardless of the port's security level) and submit it and an addendum (not the Ship Security Plan) to the COTP at the same time the Advanced Notice of Arrival is submitted or within 12 hours of the higher maritime Security Level is set by the flag administration. The addendum to the DoS (any format is acceptable) must satisfactorily address the following:

- What security functions the vessel anticipated the facility would perform at the higher security level.
- What security functions the facility has agreed to perform while remaining at the lower security level.
- What security functions the vessel will perform to compensate for functions the facility has not agreed to perform.
- What arrangements and procedures are in place to ensure that the agreed security measures between vessel and facility are being performed.

Since the regulations require the facility to determine the MARSEC Level of those vessels arriving at its facility; the facility must contact the vessel (through the agent where the vessel has engaged one), and discuss and agree upon the arrangements for the Declaration of Security and the addendum discussed above. Further, both the facility and vessel must inform the COTP about the situation and make notifications to any vessel or facility in the vicinity and any other entity (labor, bunker supplies, chandlers, and the like) that will be affected by the vessel's higher security level.

More generally, although no regulatory burden is attached, any person (pilots, labor, etc.) receiving information that a vessel is arriving at a lower security level than the port, area, or intended facility should inform the vessel master and/or vessel security officer of the higher level and the regulatory requirement to raise the vessel's security level to match that of the port or facility.

Further, owners and operators of vessels and facilities with regulatory -requires security plans who have information that a vessel is operating at a lower security level than the port or facility must report this situation as a potential security breach, see section 3420 of this plan. As discussed in section 3420, other people are not required to make these notifications, but the Federal Maritime Security Coordinator strongly encourages these people to make the reports in the interests of general security.

In some instances, a vessel may not be able to fully attain the higher security level either before making

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-3
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



arrival or for the duration of the port visit. In this case, the arriving vessel must request a COTP approval to deviate from their vessel security plan (bearing in mind SOLAS, Ch. XI-2, Regulation 9 allows the master discretion when his judgement dictates that security is compromising safety). Where a vessel is in-port at the time the MARSEC level raises, the vessel must attain the higher security level within 12 hours; when the vessel intends to depart the port before that 12 hours has elapsed, it must either assure that it will be beyond 12 nautical miles from shore and in compliance with its flag administration's directed security level, or else attain the higher level. Vessels (other than innocent passage) operating at a lower security level within 12 nautical miles of shore after the 12 hours from MARSEC level change announcement (not receipt) are considered a security breach under 33 CFR part 101. Operating at a lower security level in this circumstance may expose the vessel to Coast Guard operating and security controls and to penalty action as necessary to restore security and deter future violations. Vessels which intend to be outside the 12 nautical mile limit shortly after the 12 hour time limit expires may request approval from the COTP to deviate from the vessel's security plan.

When a vessel or multiple vessels are moored at a facility and one of the entities fails to attain the required security level within 12 hours from the time the MARSEC raise was announced, that vessel or facility is considered a security breach under 33 CFR part 101. Upon raising MARSEC, the FSO and VSOs/SSOs must complete a new Declaration of Security which outlines expected security contributions for each entity at the vessel-facility interface. When an entity fails to execute those agreed upon contributions, the other vessels (and the facility) shall take immediate corrective action to compensate for those security measures and to assure that the violating entity's security breach does not create a cascading security breach at all affected vessels and facilities. The situation must be reported as a security breach; see the reporting requirements in section 3420 of this plan.

## 4230 (U) Procedures for requesting equivalencies to MARSEC Directives

MARSEC Directives will set mandatory measures that all defined entities must meet in a specified time period. These entities will also be required to confirm, to the FMSC, receipt of the MARSEC Directive, as well as specify the method by which the mandatory measures have been (or will be) met. If a MARSEC Directive recipient is unable to implement the measures mandated in the MARSEC Directive, the recipient may propose temporary equivalent security measures to the FMSC. However, the recipient will only be able to propose such equivalencies for the shortest period of time possible never to exceed the length of the MARSEC Directive, and it will be required to implement any portion of MARSEC Directive where the FMSC does not approve a proposed equivalency. These facilities or vessels may receive verbal permission from FMSC for a temporary waiver, to be documented by the Integrated Command Center, to be followed up with documentation submitted to the FMSC within a period not to exceed six hours. See section 3400.

<b>Time allotted to comply to MARSEC Directive</b>	<b>Maximum Time required for submission of Temporary Security Measures</b>	<b>Period during which alternative or equivalent Security Measure shall remain valid.</b>
<i>12 hours</i>	<i>6 hours</i>	<i>Not to exceed length of Directive</i>

<b>VERSION DATE</b>	<b>V_1.1 26 MAY 04</b>	<b>CLASSIFICATION:</b> <b>UNCLAS / SSI</b>	<b>CONTROLLING AUTHORITY</b>	<b>USCG MSO JAX</b>	<b>ISSUING AUTHORITY</b>	<b>CAPT D.L. LERSCH</b>	<b>PAGE</b>	<b>4000-4</b>
---------------------	----------------------------	---	------------------------------	-------------------------	--------------------------	-----------------------------	-------------	---------------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Sections 104.130, 105.130, and 106.125 state that vessel or facility owners or operators requesting Alternate Security Program waivers for any requirement of part 104, 105, or 106 must include justification for why the specific requirement(s) are unnecessary for that particular owner's or operator's vessel or facility or its operating conditions. A request for a waiver must be submitted in writing with justification to the Commandant (G-MP) at 2100 Second St. SW., Washington, DC 20593.

See section 3430.2 to this plan for additional details on the handling and response to requests for waivers and equivalencies.

## 4300 (U) MARSEC Level ONE

This section is organized as follows:

- 4310 Roles, Resources, Authorities, and Responsibilities
- 4320 Standard Security Procedures for MARSEC Level ONE
- 4330 Physical Security Measures
- 4340 Operational Security (OPSEC) Measures
- 4350 Security Measures for SPOE Operations

## 4310 (SSI) Roles, Resources, Authorities, and Responsibilities

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a "covered person" under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 4320 (U) Standard Security Procedures

The Coast Guard has been designated the Lead Federal Agency for maritime homeland security. As the lead federal agency and based on the National Transportation Security Plan in 33 CFR part 102, the Coast Guard's operational commander for the eastern United States periodically issues national security classified material security procedures to tactical commanders, including the Federal Maritime Security Coordinator for Northeast and Eastern Central Florida.

The classified directives from the Coast Guard Operational Commander define certain standard security procedures which integrate the various port and coastline areas into a coherent whole, specifying certain strategies and initiatives required for the securing of the east coast as a whole. These security measures are mandatory, and may neither be disclosed nor modified without significant harm to national security.

Other Federal and State governmental agencies who are members of the Maritime Joint Task Force (MJTF) also receive standard security procedures/instructions from their operational commanders (at various national security classification levels) for the same reasons. These standard security procedures must be de-conflicted against other agency efforts (to prevent overlap, gaps, and duplication), but the security of these instructions must be carefully protected.

For this reason, the Federal Maritime Security Coordinator is seeking National Security Classified

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION:	UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-5
-----------------	--------------------	-----------------	--------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Material clearances for agency heads participating in the MJTF and with a need to participate in the tactical planning and/or deconflict of National Security Classified Material standard security measures.

At the outset of a change in Maritime Security Level (MARSEC), the Federal Maritime Security Coordinator will execute an MJTF Level TWO activation (agency head consultation) for a closed, National Security Classified tactics meeting. MJTF members with clearances, a need to know, and/or standard security measures from their own operational commanders will attend, share these standard measures to the extent necessary, design a classified force laydown executing these standard measures, identify and fill gaps in the standard security measures, and de-conflict any overlaps or duplication of effort.

## 4330 (SSI) Physical Security Measures

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a "covered person" under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

- |      |        |  |   |
|------|--------|--|---|
| (1)  | UNCLAS | FBI JTTF / FDLE<br>RDSTF / MJTF J-2  | Create a declassified single combined Northeast and Eastern Central Florida Maritime Threat Assessment at the SSI INFOSEC level and circulate to all MJTF members and all port entities required to write or update MTSA vessel or facility security plans.   |
| (22) | UNCLAS | CDC Quarantine Station, JMTF Harbor Safety Committee, USCG Captain of the Port | Designate three offshore quarantine anchorages for Jacksonville / Fernandina as holdings areas for: (1) suspected biological vectors - closest to shore; (2) suspected chemical vectors - intermediate distance offshore; and (3) suspected radiological vectors - as near the 12 NM limit as possible.   |
| (23) | UNCLAS | CDC Quarantine station and USCG Captain of the Port                            | Designate three offshore quarantine anchorages for Port Canaveral as holdings areas for: (1) suspected biological vectors - closest to shore; (2) suspected chemical vectors - intermediate distance offshore; and (3) suspected radiological vectors - as near the 12 NM limit as possible.              |
| (25) | UNCLAS | USCG   | Establish a 25 meter (100 ft) permanent no-entry security zones around all international cruiseship terminals, marine events with more than 1000 persons estimated to attend, and passenger staging areas with more than 1000 persons contained in a small shoreline area.                                |
| (26) | UNCLAS | Facility Operators and Marine/Shoreline Event Organizers                       | Establish periodic monitoring of the security zones established by measure (25); assure monitoring is low-light capable and establish hot-line procedures for emergency notification of an intrusion (from water or shore) to 911 and the Coast Guard Integrated Command Center at (904) 247-7318.        |
| (31) | UNCLAS | ALL  | Conduct annual Area Maritime Security Exercises, audits, and drills. Conduct required facility and vessel security exercises, audits, and drills under 33 CFR part 104 and 105. Periodically review the Area Plan and emergency response plans for familiarization and currency (at least once per year). |

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-6
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

(33)	UNCLAS	USCG	Halt the operation of all facilities subject to 33 CFR part 105 that do not have approved Facility Security Plans not later than 01 July 2004. Inspect facilities with approved plans for security purposes and spot - check/test security at these facilities at least once per year.
(34)	UNCLAS	USCG	Halt the operation of all vessels subject to 33 CFR part 104 that do not have approved Vessel Security Plans not later than 01 July 2004. Inspect vessels with approved plans for security purposes and spot - check/test security at these vessels at least once per year.
(35)	UNCLAS	USCG	Ban foreign vessels subject to the International Ship and Port Facility Security Code (ISPS) that do not have approved vessel security plans from U.S. waters by 01 July 2004. Inspect vessels with ISPS security plans at least once per year to verify their security plans are in place and security measures are executed in accordance with it.
(36)	UNCLAS	USCG	Conduct second-tier reviews of any vessel in violation of the Advanced Notice of Arrival regulations. Issue COTP orders to hold any vessel approaching from entering the Northeast and Eastern Central Florida ports until such time as the second-tier review of the vessel is complete. Lift the COTP order only when the vessel has screened low-risk.
(38)	UNCLAS	MJTF J-2 (Intel Squad)	Visit major marinas monthly to review activities for suspicious behavior, establish rapport, and monitor for signs of terrorist, organized crime, or illegal protest activity, logistics, or reconnaissance.
(42)	UNCLAS	All Government	Facilitate training for field-level government and private security personnel on recognizing: (1) chemical and radiological augmented IEDs; (2) routine IEDs; (3) biological vectors such as weaponized Anthrax; (4) symptoms and signs of virulent disease outbreaks (whether naturally occurring or as terrorist vectors).
(43)	UNCLAS	All	Treat all unauthorized persons / unidentified intruders as hostiles and enact CBRNE response measures (particular focus on planted CBRNE devices) until threat has been deemed non-credible (fail-safe posture).
(47)	UNCLAS	All	Maintain readiness to execute MARSEC TWO security measures in this plan and in approved facility security plans within twelve (12) hours. Review MARSEC TWO security measures in this plan and approved VSPs/FSPs at least once per quarter.

## 4340 (SSI) Operational Security (OPSEC) Measures

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-7
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

(O-4)	UNCLAS	All	Minimize to the extent possible budgetary limitations related to security measures, systems, and forces are made public.
(O-5)	UNCLAS	All	Protect the security training status and records of personnel – make it difficult to learn who has completed what training and for what purpose they were trained.
(O-6)	UNCLAS	All	Avoid descriptive or easily associated project names and exercise names, acronyms, and nicknames in conducting security business.
(O-7)	UNCLAS	All	Periodically conduct surveillance of your own property and/or operation and identify signals/patterns/indicators that alert observers when you are about to conduct specific critical operations (e.g., pier lights always energized ½ hour before vessels arrive), and re-design so that these indicators are used for a variety of operations and periodically employed when no operation is on-going, thereby eliminating their value as true indicators for adversary surveillance.
(O-9)	UNCLAS	All	Review web-sites and public calendars that would indicate locations/schedules/activities of executives and critical personnel and remove these sites.

## 4350 (SSI) Security Measures for SPOE Operations

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 4400 (U) MARSEC Level 2

This section is organized as follows:

- 4410 Roles, Resources, Responsibilities
- 4420 Standard Security Procedures for MARSEC Level TWO
- 4430 Physical Security Measures
- 4440 Operational Security Measures
- 4450 Security Measures for SPOE Operations

## 4410 (SSI) Roles, Resources, Authorities, and Responsibilities

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-8
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4420 (U) Standard Security Procedures for MARSEC Level TWO

The Coast Guard has been designated the Lead Federal Agency for maritime homeland security. As the lead federal agency and based on the National Transportation Security Plan in 33 CFR part 102, the Coast Guard's operational commander for the eastern United States periodically issues national security classified material security procedures to tactical commanders, including the Federal Maritime Security Coordinator for Northeast and Eastern Central Florida.

The classified directives from the Coast Guard Operational Commander define certain standard security procedures which integrate the various port and coastline areas into a coherent whole, specifying certain strategies and initiatives required for the securing of the east coast as a whole. These security measures are mandatory, and may neither be disclosed nor modified without significant harm to national security.

Other Federal and State governmental agencies who are members of the Maritime Joint Task Force (MJTF) also receive standard security procedures/instructions from their operational commanders (at various national security classification levels) for the same reasons. These standard security procedures must be de-conflicted against other agency efforts (to prevent overlap, gaps, and duplication), but the security of these instructions must be carefully protected.

For this reason, the Federal Maritime Security Coordinator is seeking National Security Classified Material clearances for agency heads participating in the MJTF and with a need to participate in the tactical planning and/or deconflict of National Security Classified Material standard security measures.

At the outset of a change in Maritime Security Level (MARSEC), the Federal Maritime Security Coordinator will execute an MJTF Level TWO activation (agency head consultation) for a closed, National Security Classified tactics meeting. MJTF members with clearances, a need to know, and/or standard security measures from their own operational commanders will attend, share these standard measures to the extent necessary, design a classified force laydown executing these standard measures, identify and fill gaps in the standard security measures, and de-conflict any overlaps or duplication of effort.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-9
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



## 4430 (SSI) Physical Security Measures

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

- (94) UNCLAS All Continue all MARSEC ONE Security Measures except measures (31), (32), (38), and (42).
- (95) UNCLAS All vessels and facilities with required security plans, all government installations **Conduct an OPERATIONAL PAUSE** while all spaces and operations ashore and afloat are reviewed. Ongoing operations need not be halted, but all operations should be reviewed and all spaces/areas/compartments should be checked. Do not start new operations/transits until all-clear is confirmed by the FSO/VSO. Report the all-clear as soon as possible and no later than two hours after notification to the USCG Integrated Command Center, **3440.2**. Report suspicious activity or security breaches to 911 and the National Response Center at (800) 424-8802. For entities with approved facility or vessel security plans, begin implementing MARSEC TWO security measures after the operational pause is complete and confirm attainment of MARSEC TWO within twelve hours. Report inability (shortfalls) to attain elements of MARSEC TWO security measures immediately to the USCG Integrated Command Center. Repeat review/search procedures every 24 hours while MARSEC TWO is maintained, including report of "all clear" to the Integrated Command Center, **3440.2**.
- (97) UNCLAS USCG Captain of the Port Issue/activate Security Zone regulations and Broadcast Notices to Mariners requiring all pilots and operators of vessels over 50 meters in length (tug operators for barges over 50 meters in length) intending to transit the following areas to contact and clear with the Coast Guard/MJTF vessel serving as Sentinel/Gate-keeper offshore before making inbound or outbound transits: (1) St. Marys River and the ICW from Kings Bay to the ocean and three miles around the mouth to the St. Marys River; (2) St. Johns River from Dames Point Cruise Terminal to the ocean and three miles around the mouth to the St. Johns River; (3) Port Canaveral and three miles around the entry to Port Canaveral; and (4) all federal anchorages as defined in 33 CFR 110.183.
- (99) UNCLAS USCG Captain of the Port Upon MARSEC TWO set, issue a general Captain of the Port order requiring the conduct of **Operational Pause** searches of all vessels over 50 meters in length, and the report of “all clear” to the Coast Guard Integrated Command Center. Lift the general Captain of the Port Order only when the large majority of vessels and facilities requiring security plans have reported all-clear.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-10
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- (100) UNCLAS Owners of properties located within 100 meters of a bridge over the Intercoastals Waterway, St. Johns River, Banana River, or Indian River Upon MARSEC TWO set, review all operations on your property or by tenants on your property as part of the Operational Pause and conduct a search of your property for unauthorized vehicles and/or placed packages/bins/containers which could be Improvised Explosive Devices (IEDs) endangering the bridge and/or its supports. Report suspicious vehicles and packages to the police at 911 and the Coast Guard Integrated Command Center (904) 247-7318. Report the all-clear to the Coast Guard Integrated Command Center (see paragraph **3440.2**) as soon as possible and in no case more than two hours after MARSEC TWO set. Conduct a similar search/review at least once every 48 hours and report the all-clear to the Coast Guard Integrated Command Center.
- (101) UNCLAS Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons Upon MARSEC TWO set, review all operations on your property or by tenants on your property as part of the Operational Pause and conduct a search of your property for unauthorized vehicles and/or placed packages/bins/containers which could be Improvised Explosive Devices (IEDs) endangering the areas where people congregate. Report suspicious vehicles and packages to the police at 911 and the Coast Guard Integrated Command Center at (904) 247-7318. Report the all-clear to the Coast Guard Integrated Command Center (see paragraph **3440.2**) as soon as possible and in no case more than two hours after MARSEC TWO set. Conduct a similar search/review at least once every 48 hours and report the all-clear to the Coast Guard Integrated Command Center.
- (103) UNCLAS Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons Limit the total number of people attending your events / congregating and/or disperse people in your buildings/attending events/congregating such that the density of persons limits the number of people to 1000 within a 25 meter radius, thereby limiting the consequences of an Improvised Explosive Device attack by limiting the number of people inside IED stand-off distance. Review and remove as much as possible anything that is likely to serve as secondary debris for an IED detonated anywhere within your event/congregation area/building. To the extent possible, re-locate congregation areas/high-density areas away from exterior walls and windows thereby reducing vulnerability to IEDs detonated in proximity to outsides of building and reducing flying debris impacts.
- (104) UNCLAS Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons Review and limit as much as possible the number of vehicle access points to your event, building, or passenger staging area. Limit vehicle approaches to 10 meters of congregation/inhabited areas. Because the energy of an approaching vehicle (laden or unladen with explosives) increases with the square of the speed of the vehicle, increase the stand-off distances to congregation areas in the direct path of high-speed approaches (straight-on streets, etc.). Wherever possible move congregation areas, etc., into areas at a tangent to high-speed approaches. Minimize vehicle speeds in areas under your control. Conduct IED sweeps on all vessels coming alongside prior to approach, particularly on passenger vessels, while passengers are present (bunker when passengers are not present).

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-11
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- (105) UNCLAS Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons Review likely vantage points for terrorist, organized crime, and illegal protest surveillance of your buildings, congregation areas, and vehicle or pedestrian access points, even when those vantage points are outside your area of control. To the extent possible, place obstructions and screens to reduce visibility of your operations/event/areas from those likely vantage points.
- (109) UNCLAS FL National Guard Civil Support Team Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
- (110) UNCLAS Florida Department of Health Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
- (111) UNCLAS USN Commander, Navy Region Southeast Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
- (112) UNCLAS Commanding General, Patrick Air Force Base and Director Kennedy Space Center Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
- (113) UNCLAS MJTF Liason Officer Initiate and maintain close liaison with CDC Quarantine Station in Miami.
- (114) UNCLAS MJTF Deploy liaison officer assistants to the Brevard, Duval, and Nassau County Emergency Operations Centers (MACCs within the National Response Plan framework) for interagency coordination outside the Marine division. All federal, state, and local governmental marine entities will be integrated into MJTF Unified Command and represented as assigned within the MTJF ICS.
- (115) UNCLAS MTJF Deploy liaison officer assistants to the FBI Emergency Operations Center and FDLE Emergency Operations Center if activated.
- (117) UNCLAS USCG Captain of the Port Maintain and continuously track through the MTJF-ICC all shortfalls reported by facilities and vessels with approved security plans. Evaluate shortfalls and where shortfalls create a manifestly unsafe condition in view of MARSEC TWO Threat Information, issue Captain of the Port Orders halting operations and/or closing the security shortfall. Where MJTF resources/efforts are required to close the gap, assign same as a priority to the MJTF Unified Command. Update and include gap-closing measures in the Common Tactical Picture (CTP) and coordinate continued MJTF reconnaissance on shortfalls where necessary to evaluate required gap-closing security measures.
- (118) UNCLAS USCG Captain of the Port Issue/activate RNA regulations and Broadcast Notices to Mariners forbidding mooring to or loitering in the vicinity of all bridges over the ICW, St. Marys River, St. Johns River, Banana River, Indian River, Barge Canal (Canaveral), and Hanover Canal.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-12
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- (125) UNCLAS MJTF, Facility Operators and Marine/Shoreline Event Organizers Increase monitoring of security zones around terminals and high-density marine/shoreline events defined in MARSEC ONE Security Measure (25) to continuous low-light capable monitoring plus periodic patrols by security personnel (from ashore acceptable) on a randomly-timed, randomly-rotating frequency of patrol basis.
- (131) UNCLAS USCG Captain of the Port Within 24 hours of MARSEC TWO set, hold open-session Port Security Committee meetings in Jacksonville/Fernandina and Port Canaveral to refresh all personnel on this plan, MARSEC TWO security measures, recognition of CBRNE vectors and devices, and the specific threat information.
- (133) UNCLAS USCG and FDEP Within 24 hours of MARSEC TWO set, alert all pollution response contractors to attain heightened deployment readiness. Review Area Contingency Plan, Hazardous Materials Annex, and County Disaster Response Plans.
- (134) UNCLAS USCG, FWCC, and FDLE Deploy auxiliary support officers throughout boating community at marinas stores, dives shops, etc., to assure maximum awareness of MARSEC TWO security zones, restrictions, and issues. Maintain continuous effort throughout MARSEC TWO.
- (135) UNCLAS All Maintain readiness to execute MARSEC THREE security measures in this plan and in approved facility security plans within twelve (12) hours. Review MARSEC THREE security measures in this plan and approved VSPs/FSPs within six hours of MARSEC TWO set.

## 4440 (SSI) Operational Security Measures

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

- (O-11) UNCLAS All Continue all MARSEC ONE and OPSEC Measures except (O-1), (O-3), (O-8), (O-9), and (O-10).
- (O-12) UNCLAS All Schedule operations and activities simultaneously so they mask each other and confuse observers as to what is happening and how the operations are related (if at all).
- (O-15) UNCLAS All Disrupt anyone who might be monitoring/surveillance your operations by occasionally rotating your communications procedures (from radio to cell phone to land-line) etc.
- (O-16) UNCLAS MJTF Within four hours of MARSEC TWO set, begin monitoring of OPSEC measures within the port and on vessels. Assure vessels, facilities, and other marine areas are using these OPSEC measures and those defined within their own security plans.
- (O-19) UNCLAS All Gradually change your activity levels to meet MARSEC TWO requirements so the change is less apparent; gradually slow your activity levels after “operational pause” that the observers will not readily understand when the operational pause has ceased.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-13
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

(O-20)	UNCLAS	All commercial entities	Without disrupting operations, time activities to occur during periods of least security vulnerability,e.g. avoid scheduling delivery of stores during passenger embarkation.
(O-24)	UNCLAS	All	To the extent possible, change the critical personnel reporting times and operational cycles in order to maximize adversary confusion. Vary the times and routes by which all executives and critical personnel report to work.
(O-25)	UNCLAS	All	Minimize the use of e-mail and web pages to convey information about operational schedules, vessel arrival and departure times, and so on. Password protect fee-for-service web pages with vessel arrival and operational information.

## 4450 (SSI) Security Measures for SPOE Operations

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 4500 (U) MARSEC Level 3

This section is organized as follows:

- 4510 Roles, Resources, Authorities, and Responsibilities
- 4520 Standard Security Procedures for MARSEC Level THREE
- 4530 Physical Security Measures
- 4540 Operational Security (OPSEC) Measures
- 4550 Security Measures for SPOE Operations

## 4510 (SSI) Roles, Resources, Authorities, and Responsibilities

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-14
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4520 (U) Standard Security Procedures for MARSEC Level THREE

The Coast Guard has been designated the Lead Federal Agency for maritime homeland security. As the lead federal agency and based on the National Transportation Security Plan in 33 CFR part 102, the Coast Guard's operational commander for the eastern United States periodically issues national security classified material security procedures to tactical commanders, including the Federal Maritime Security Coordinator for Northeast and Eastern Central Florida.

The classified directives from the Coast Guard Operational Commander define certain standard security procedures which integrate the various port and coastline areas into a coherent whole, specifying certain strategies and initiatives required for the securing of the east coast as a whole. These security measures are mandatory, and may neither be disclosed nor modified without significant harm to national security.

Other Federal and State governmental agencies who are members of the Maritime Joint Task Force (MJTF) also receive standard security procedures/instructions from their operational commanders (at various national security classification levels) for the same reasons. These standard security procedures must be de-conflicted against other agency efforts (to prevent overlap, gaps, and duplication), but the security of these instructions must be carefully protected.

For this reason, the Federal Maritime Security Coordinator is seeking National Security Classified Material clearances for agency heads participating in the MJTF and with a need to participate in the tactical planning and/or deconflict of National Security Classified Material standard security measures.

At the outset of a change in Maritime Security Level (MARSEC), the Federal Maritime Security Coordinator will execute an MJTF Level TWO activation (agency head consultation) for a closed, National Security Classified tactics meeting. MJTF members with clearances, a need to know, and/or standard security measures from their own operational commanders will attend, share these standard measures to the extent necessary, design a classified force laydown executing these standard measures, identify and fill gaps in the standard security measures, and de-conflict any overlaps or duplication of effort.

## 4530 (SSI) Physical Security Measures

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a "covered person" under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-15
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(174)	UNCLAS	All	Continue all MARSEC ONE and TWO Security Measures except measures (31), (32), (38), and (42).
(175)	UNCLAS	All vessels and facilities with required security plans, all government installations	<b>Conduct OPERATIONAL PAUSE</b> as defined in MARSEC TWO Security Measure (95). Upon receiving notification of MARSEC THREE set, conduct an operational pause while all spaces and operations ashore and afloat are reviewed. No vessels are to depart the dock or make entry into the port. Re-start operations after all-clear is confirmed by the FSO/VSO. Report the all-clear as soon as possible and no later than two hours after notification to the USCG Integrated Command Center, <b>3440.2</b> . Report suspicious activity or security breaches to 911 and the National Response Center at (800) 424-8802. For entities with approved facility or vessel security plans, begin implementing MARSEC THREE security measures after the operational pause is complete and confirm attainment of MARSEC THREE within twelve hours. Report inability (shortfalls) to attain elements of MARSEC THREE security measures immediately to the USCG Integrated Command Center. Repeat review/search procedures every 12 hours while MARSEC THREE is maintained, including report of "all clear" to the Integrated Command Center, <b>3440.2</b> .
(176)	UNCLAS	USCG Captain of the Port	Upon MARSEC THREE set, issue a Captain of the Port order as defined in MARSEC TWO Security Measure (99) prohibiting the entry and departure of vessels except law enforcement and emergency response as part of the Operational Pause. Ban all recreational vessels on the St. Johns River from the I-295 bridge to the Ocean, on the St. Marys River and ICW from Kings Bay to the ocean, and in Port Canaveral for the duration of MARSEC THREE. Once an all-clear has been reported, grant permission for the vessel to resume operations, and lift the Captain of the Port Order only when the large majority of vessels and facilities requiring security plans have reported all-clear. Incoming vessels that cannot divert to another port must be queued and escorted to the dock, <b>3440.2</b> .
(179)	UNCLAS	ALL	Queue all commercial traffic entering or leaving the St. Johns River, St. Marys River, and Port Canaveral using the Sentinel / Gate-keeper as traffic control. Contact the Gate-keeper via VHF 21A for queuing information.
(183)	UNCLAS	All Operators	Implement MARSEC TWO Security Measures (103), (104), (105) and (106) to the maximum extent possible.
(191)	UNCLAS	All	Review security incident response plans and refresh all personnel on procedures contained therein. Place any specialized personnel and/or equipment required in stand-by status for maximum speed of response.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-16
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4540 (SSI) Operational Security Measures

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

(O-27)	UNCLAS	All	Continue all MARSEC ONE and TWO OPSEC Measures except (O-1), (O-3), (O-8), (O-9), and (O-10)
(O-28)	UNCLAS	MJTF	Within one hour of MARSEC THREE set, begin monitoring of OPSEC measures within the port and on vessels. Assure vessels, facilities, and other marine areas are using these OPSEC measures and those defined within their own security plans.
(O-30)	UNCLAS	All	To the extent possible, change the shift reporting times and operational cycles in order to maximize adversary confusion. Vary the times and routes by which all employees report to work, and consider staggered arrival times within one shift.

## 4550 (SSI) Security Measures for SPOE Operations

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 4600 (U) Public Access Facility

A Public Access Facility (PAF) is defined in regulation at 33 CFR 101.105. A PAF is an area with public access that is primarily used for recreation or entertainment purposes, not the reception or servicing of vessels regulated under 33 CFR part 104. This may include a public pier, wharf, dock, waterside restaurant, or marina that contains minimal maritime infrastructure such as bollards, cleats, or ticket booths.

For a location to be designated a PAF, it must meet all three of the elements of the definition: (1) it must be used by the public, primarily for recreation, entertainment, retail, or tourism; not for receiving vessels regulated under 33 CFR part 104; (2) it must have minimal infrastructure for servicing vessels subject to 104, particularly with regard to cargo operations; and (3) it must not receive vessels which are regulated by 33 CFR 104 other than ferries permitted to carry vehicles; cruise ships; or other passenger vessels subject to the SOLAS Convention, Chapter XI.

For instance, a marina restricting access to its piers and receiving regulated vessels other than ferries,

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-17
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

cruise ships, or SOLAS passenger vessels may not be considered a PAF, nor would a city dock with minimal infrastructure receiving a cargo vessel. Conversely, where docks are used for a vehicle ferry and are open to the public, the facility may apply for PAF status.

## 4610 (U) Designation of Public Access Facilities (PAF)

This section outlines the process by which a facility or structure is designated by the Federal Maritime Security Coordinator as a Public Access Facility (PAF). This section is organized as follows:

- 4611 PAF Exemption Request
- 4612 Review and Evaluation of PAF Exemption Request
- 4613 Establishment of Conditions
- 4614 Issuance of PAF Designation

As of 01 April 2004, the Captain of the Port has not designated any Public Access Facilities in Northeast or Eastern Central Florida. Tab D to Appendix 9940 is reserved for publicly accessible listings of any PAFs designated by the Captain of the Port in the future.

### 4611 (U) PAF Exemption Request

The owner or operator of a facility seeking exemption from 33 CFR part 105 may request to the cognizant Captain of the Port designation as a Public Access Facility (PAF). As per 33 CFR 101.105, the definition of a PAF is an area with public access that is primarily used for recreation or entertainment purposes, and which primary purpose does not include receiving or servicing of vessels regulated under 33 CFR 104. This may include a public pier, wharf, dock, waterside restaurant or marina that contains minimal infrastructure such as only bollards, cleats, or ticket booths. Applicants are free to submit the request for exemption in whatever format or venue they elect, but the information contained in the sample PAF Exemption Request (TAB A to Appendix 9940) will be required in order for the Captain of the Port to take initial review action. Where the information submitted is insufficient in the Captain of the Port's view, he or she may request additional information in writing. Requests for Exemption / Designation as a PAF should be made in writing to:

Commanding Officer  
USCG Marine Safety Office  
ATTN: Facilities Branch  
7820 Arlington Expressway, Suite 400  
Jacksonville, FL 32211

### 4612 (U) Review and Evaluation of PAF Exemption Request

The Captain of the Port will conduct a complete review of each PAF Exemption Request. This review and evaluation will consider the information submitted along with the results and impacts to the overall security of the port as documented in the Area Maritime Security Assessment Report.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION:	UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-18
-----------------	--------------------	-----------------	--------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Depending upon the complexity of the site and the information available, the Captain of the Port may conduct an on-site evaluation to evaluate elements of the request and validate claims about the common usage of the structure.

Where the Captain of the Port determines the facility does not meet the definition of a Public Access Facility, the Captain of the Port will inform the applicant in writing the exemption request has been denied. The facility remains bound by the requirements of 33 CFR part 105 if the PAF exemption request is denied.

## 4613 (U) Establishment of Conditions

Once the Captain of the Port has determined that an applicant facility or structure does in fact meet the definition of a PAF, he or she will coordinate with the owner or operator of the facility to establish the conditions under which this exemption from part 105 will be given. Mandatory security measures for all PAFs in MARSEC ONE, TWO, and THREE are detailed in TAB B to Appendix 9940. All PAFs, regardless configuration or use, must meet these mandatory security measures. Additionally, the Captain of the Port may impose security measures from those listed as “additional” in TAB B to Appendix 9940 in view of action necessary to control the risk at the PAF to acceptable levels.

## 4614 (U) Issuance of PAF Designation

After the Captain of the Port has evaluated the facility and determined which security measures must be applied at the PAF, the Captain of the Port will document both the mandatory and additional security measures which the PAF must institute in a letter designated the facility or structure as a PAF. Security conditions will be included as an enclosure to the designation letter, and are considered Sensitive Security Information under 49 CFR part 1520. See section 3500 of this plan for further information on the handling and protection of Sensitive Security Information.

Once the PAF owner or operator receives the written PAF designation, he or she must acknowledge receiving this designation to the Captain of the Port; the designation is considered effective upon the owner or operator’s acknowledgement. The acknowledgement must contain the name and 24-hour contact number of the individual with security responsibilities for the PAF. The Captain of the Port will keep a copy of the designation letter and acknowledgement letter as a permanent attachment to this AMS plan (see TAB C to Appendix 9940) until the facility’s designation is revoked. The PAF designation and list of applicable security measures will be reviewed by the Captain of the Port once each year to assure the exemption remains appropriate.

Any contemplated change to a PAF’s infrastructure or operation must be reported to the Captain of the Port immediately so that he or she may determine whether the facility must be re-evaluated as a PAF in light of the changes.

## 4620 (U) Vessel Responsibilities when Calling at a PAF

This section outlines the responsibilities of vessels subject to 33 CFR part 104 when making calls at a Public Access Facility (PAF). This section is organized as follows:

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-19
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- 4621 General Responsibilities
- 4622 MARSEC ONE Responsibilities
- 4623 MARSEC TWO Responsibilities
- 4624 MARSEC THREE Responsibilities

## 4621 (U) General Responsibilities

Vessels subject to 33 CFR part 104 must assure their Vessel Security Plans address security concerns while the vessel is at the PAF, per 33 CFR 104.292(d).

Vessels subject to 33 CFR part 104 must implement all appropriate security measures while at the PAF, however, they may liaison with the PAF to determine who will actually perform security activities.

## 4622 (U) MARSEC ONE Responsibilities

At MARSEC ONE, the owner/operator of a vessel subject to 104, or the VSO/CSO, must contact the individual with security responsibilities for the PAF prior to their first visit to determine which security measures will be in place at the PAF. Appendix 9940 to this plan lists the PAFs designated by the Captain of the Port.

A vessel subject to 33 CFR part 104 but frequently interfacing with the same PAF must also contact the Individual with security responsibilities for the PAF whenever there is a significant change in operations.

Whenever a vessel subject to 33 CFR part 104 is unable to contact the individual with security responsibilities for the PAF prior to arrival, the vessel VSO must assume responsibility for all security activities, and must notify the Captain of the Port.

## 4623 (U) MARSEC TWO Responsibilities

At MARSEC TWO, the owner/operator of a vessel subject to 33 CFR part 104, or the VSO/CSO, must contact the individual with security responsibilities at the PAF and execute a Declaration of Security (DoS) prior to each visit to determine the security measures which will be in place at the PAF.

A vessel subject to 33 CFR part 104 that frequently interfaces with the same PAF may execute a continuing DoS for multiple visits provided the effective period of the DoS is not more than 30 days. Whenever a vessel subject to 33 CFR part 104 is unable to contact the individual with security responsibilities for the PAF prior to arrival, the vessel VSO must assume responsibility for all security activities, and must notify the Captain of the Port.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-20
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 4624 (U) MARSEC THREE Responsibilities

At MARSEC THREE, the owner/operator of a vessel subject to 33 CFR part 104, or the VSO/CSO, must contact the individual with security responsibilities at the PAF and execute a Declaration of Security (DoS) prior to each visit to determine the security measures which will be in place at the PAF.

Continuing DoS are not authorized for use at PAFs during MARSEC THREE.

Whenever a vessel subject to 33 CFR part 104 is unable to contact the individual with security responsibilities for the PAF prior to arrival, the vessel VSO must assume responsibility for all security activities, and must notify the Captain of the Port.

## 4630 (U) Compliance and Enforcement

This section outlines the general compliance and enforcement posture related to Public Access Facilities). This section is organized as follows:

- 4631 Submission of PAF Exemption Requests
- 4632 Action on Requests
- 4633 Annual Review
- 4634 Enforcement Action

### 4631 (U) Submission of PAF Exemption Request.

(1) Facilities that were in operation on or before December 31, 2003 should have submitted a Facility Security Plan (FSP) and a request for PAF Exemption/designation prior to January 01, 2004.

(2) Facilities that have submitted an FSP and wish to be considered for exemption/designation as a PAF prior to July 01, 2004 must submit an exemption request to the Captain of the Port at least 60 days prior to the requested designation date. The facility must be designated a PAF by the Captain of the Port before it may operate as one.

(3) Facilities operating under an approved FSP that wish to be considered for exemption/designation as a PAF after July 01, 2004 must submit a request to the Captain of the Port at least 60 days prior to the requested designation date. The facility must continue to operate under the FSP until designated a PAF by the Captain of the Port.

(4) Facilities not in operation before December 31, 2003 that wish to be considered for designation as a PAF must submit a request for exemption/designation as a PAF to the Captain of the Port no later than 60 days prior to beginning operation. The facility must be designated a PAF by the Captain of the Port before it may operate as one. Facilities requesting designation as a PAF must comply with the Facility Security Plan submission requirements at 33 CFR 105.410(b) – i.e., 60 days prior to beginning operations – until such time as the PAF designation is granted.

(5) If a facility has a change of ownership, the individual with security responsibilities must submit

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION:	UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-21
-----------------	--------------------	-----------------	--------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



updated contact information to the Captain of the Port. The owner/operator of a PAF must conduct a review of the PAF designation and notify the Captain of the Port of any changes to the facility's operations that may affect security. The new owner/operator or individual with security responsibilities must sign an acknowledgement of the PAF designation and conditions/security measures.

## 4632 (U) Action of Requests

After receiving an Exemption Request, the Captain of the Port will:

- approve the request with conditions via a PAF Designation Letter;
- request additional information to make a determination; or
- deny the exemption request with a letter restating the requirements of 33 CFR 105 (or stating that the facility is not subject to the requirements of 33 CFR 105).

## 4633 (U) Annual Review

The Captain of the Port will review each PAF exemption / designation annually to assure the exemption remains appropriate.

Any changes to the operations or description of the facility must be immediately reported by the PAF owner/operator or individual with security responsibilities to the Captain of the Port. Anticipated changes should be reported in writing to:

Commanding Officer  
USCG Marine Safety Office  
ATTN: Facilities Branch  
7820 Arlington Expressway, Suite 400  
Jacksonville, FL 32211

## 4634 (U) Enforcement Actions

In general, the Federal Maritime Security Coordinator anticipates non-compliance with the PAF exemption to consist of:

- Incorrect contact information for the individual with security responsibilities;
- The PAF temporarily cannot institute/maintain one or some of the required conditions / security measures attached to the PAF designation letter; or
- The PAF chronically or always fails to implement a majority of the required conditions / security measures attached to the PAF designation letter.

Coast Guard enforcement actions will vary according to the nature of the non-compliance and the remedial action taken by the PAF owner/operator. Options available to the Federal Maritime Security Coordinator (in no particular order) include:

- informal request for immediate correction or update of administrative information;
- a formal letter from the Captain of the Port requesting correction of the discrepancy within a

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION:	UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-22
-----------------	--------------------	-----------------	--------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- specified and reasonable timeframe;
- a Captain of the Port Order suspending operation with vessels subject to 33 CFR part 104 until satisfactory evidence of compliance with the PAF designation conditions / security measures is presented and accepted;
- an administrative civil penalty; or
- a letter revoking the facility's designation as a PAF and requiring full compliance with 33 CFR part 105, usually accompanied by a Captain of the Port Order specifying the conditions under which the facility may operate until the facility's new FSP is approved.

## 4700 (U) Maritime Worker Credentials

Any personal identification credential for maritime workers accepted under the access control provisions of 33 CFR 101, Chapter 1, Subchapter H must, at least, meet the following requirements:

1. Be laminated or otherwise secure against tampering.
2. Contain the individual's full name.
3. Contain a photo which depicts the individual's current facial appearance.
4. Bear the name of the issuing authority.

The issuing authority must be a government authority, an organization authorized to act on the behalf of a government authority, or the individual's employer, union, or trade association.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-23
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 5000 PREPAREDNESS FOR RESPONSE

This section details how the Northeast and Eastern Central Florida area has prepared to respond to security incidents. The section is organized as follows:

- 5100 [Introduction](#)
  - 5110 [Procedures for Responding to Suspicious Activity](#)
  - 5120 [Procedures for Responding to Breaches in Security](#)
- 5200 [Transportation Security Incidents](#)
  - 5210 [Procedures for Notifying](#)
  - 5220 [Incident Command System Activation](#)
- 5300 [Most Probable Transportation Security Incidents](#)
  - 5310 [Unified Command Assignments](#)
  - 5320 [Procedures for Responding to Transportation Security Incidents](#)
  - 5330 [Linkage to Applicable Federal, State, Port and Local Plans](#)
- 5400 [Maritime Security Exercise Requirements](#)
  - 5410 [Purpose of the AMS Exercise Program](#)
  - 5420 [Goals of the AMS Exercise Program](#)
  - 5430 [Cycle of Exercises](#)
  - 5440 [Scheduling and Design](#)
  - 5450 [Consideration of Equivalent Response](#)
  - 5460 [Recordkeeping](#)
  - 5470 [Linkages between the Family of Plans](#)

### 5100 (U) Introduction

This section outlines the procedures for reporting and responding in Northeast and Eastern Central Florida to Suspicious Activities and Security Breaches, neither of which necessarily rises to the level of a Transportation Security Incident. The section provides guidelines both to the Maritime Joint Task Force and to the general port (private and commercial vessels, facilities, and infrastructure owners). The section is organized as follows (click the link to view the sub-section):

- 5110 [Procedures for Responding to Suspicious Activity](#)
- 5120 [Procedures for Responding to Security Breaches](#)

### 5110 (SSI) Procedures for Responding to Suspicious Activity

This section defines the procedures for responding to a report of suspicious activity occurring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific Suspicious Activities for which the Port Security Committee has developed response procedures for three general scenarios. These procedures include unclassified guidelines for the port community and Security Sensitive Information procedures for the Maritime Joint Task Force. Continued development of these Annexes will include Geographically -Specific TSI Response Action Procedures (GSTRAP). The two suspicious activity scenarios include:

- (SA-1) Bomb Threat ([UNCLAS Annex](#))
- (SA-2) Access Attempt, Suspicious Boating, Suspicious Divers

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION:	UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-1
-----------------	--------------------	-----------------	--------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

(UNCLAS Annex)  
(SA-3) Photos / Surveillance (UNCLAS Annex)

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 5120 (U) Procedures for Responding to Breaches in Security

This section defines the procedures for responding to a breach of security occurring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific breaches of security for which the Port Security Committee has developed response procedures for four general scenarios. These procedures include unclassified guidelines for the port community and Security Sensitive Information procedures for the Maritime Joint Task Force. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The four security breach scenarios include:

- (SB-1) Trespass Ashore, Stowaway Discovered, or Smallboat in Security Zone  
(UNCLAS Annex)
- (SB-2) Small-scale illegal demonstration (UNCLAS Annex)
- (SB-3) Evidence of Tampering w/ Security Systems (UNCLAS Annex)
- (SB-4) Security Measures Not in Place (UNCLAS Annex)

See Table 5110.1 for expected on-scene response timeframes to major port areas.

## 5200 (U) Transportation Security Incident (TSI)

All port entities (government, commercial, and recreational) must report a TSI immediately to the appropriate emergency responders (dial 911) and then to the local Federal Maritime Security Coordinator (dial 904-247-7318 for the Coast Guard Integrated Command Center) and the National Response Center (dial 1-800-424-8802).

There will be threats, causes for concern, and violations of existing security plans that are worth investigation, but do not rise to the level of a TSI. This could be due to simple-miscommunications, lost credentials, an innocent person unaware of entry restrictions or perimeters, etc. In most of these cases, simple resolution of the problem or referral to appropriate authorities is the only action needed. Incidents that highlight serious discrepancies within required plans shall be reported to the FMSC (see section 5100).

Examples of events not requiring TSI notification:

- Lost or expired credentials.
- Mis-delivered cargo or passengers.
- Simple trespassing. See section 5120, SB-1
- Minor incident that temporarily disrupt the MTS system, such as authorities investigating a broken down vehicle.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-2
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

- Misdemeanors on a public facility, such as fights, public intoxication.
- Violations of company policies not directly related to security.

See Table 5110.1 for expected on-scene response timeframes to major port areas.

## 5210 (U) Procedures for Notification

A TSI must first be reported to the appropriate emergency services (dial 911) to ensure human health and safety measures are taken. Secondary notifications must be made to the Coast Guard Federal Maritime Security Coordinator (dial 904-247-7318 for the Coast Guard Integrated Command Center), then to the National Response Center (dial 1-800-424-8802).

## 5220 (U) Incident Command Activation

The Federal Maritime Security Coordinator, normally in consultation with partner agencies, will determine the need to establish an incident command or unified command for a particular incident. In general, all incidents are managed (even when limited resources of a single agency are involved) under the National Incident Management System (NIMS) as directed in Homeland Security Presidential Directive Number Five (HSPD-5). The designated incident commander for each responding agency, whether patrolman or more senior, is responsible for forming a Unified Command with other agency Incident Commanders on-scene. The NIMS is an expandable system, with activation being determined by the needs of operations on-scene.

Where the incident clearly will require extensive management, the FMSC may elect any one of the following levels of Incident Command Activation:

- (1) **MJTF Notification and Monitoring.** Through the Coast Guard Integrated Command Center, the FMSC may elect to notify all MJTF member agencies (i.e., potential unified command members) of an incident, and continue to monitor the progress of that incident on behalf of the MJTF member agencies.
- (2) **MJTF Unified Command Activation Only.** Through the Coast Guard Integrated Command Center, the FMSC may elect to consult with MJTF Unified Commanders (agency heads) only, without formally or fully activating joint operations and management of the incident.
- (3) **Full MJTF Activation.** Through the Coast Guard Integrated Command Center, the FMSC may elect to proceed directly to full activation of MJTF command and operations for a significant incident under the National Incident Management System.

Specific decision points regarding the Unified Command consultations and MJTF activation under the National Incident Management System (NIMS) are outlined in the Sensitive Security Information MJTF annexes to section 5320 below.

## 5230 (U) Threats that Do Not Rise to the Level of a TSI

There will be threats, causes for concern, and violations of existing security plans that are worth investigation, but do not raise to the level of a TSI. This could be due to simple-miscommunications, lost credentials, an innocent person unaware of entry restrictions or perimeters, etc. In most of these cases, simple resolution of the problem or referral to the authorities as suspicious activity or a security breach is the only action needed. Incidents that reveal serious discrepancies or weaknesses within the required vessel and facility security plans must be reported to the Federal Maritime Security

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-3
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Coordinator as discussed in section 5110 and 5120 of this plan.

## 5300 (SSI) Most Probable Transportation Security Incident

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 5310 (U) Unified Command Assignments

In general, organization of responses to Transportation Security Incidents in Northeast Florida and Eastern Central Florida will be governed by the standard or suggested organizations applicable to the event as outlined in the Coast Guard’s Incident Management Handbook. Specific Unified Command assignments for MJTF member agencies are outlined in each of the Sensitive Security Information Response Procedure Annexes outlined in section 5320.

## 5320 (U) Procedure for responding to TSI

This section defines the procedures for responding to a Transportation Security Incident occurring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific TSIs for which the Port Security Committee has developed response procedures for eleven specific scenarios. These procedures include unclassified guidelines for the port community and Security Sensitive Information procedures for the Maritime Joint Task Force. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The eleven Transportation Security Incident scenarios include:

- (TSI1) Rogue Vessel (UNCLAS Annex)
- (TSI2) CBR Terrorism (UNCLAS Annex)
- (TSI3) Explosive Device Discovery (UNCLAS Annex)
- (TSI4) Armed Trespass (UNCLAS Annex)
- (TSI5) Suspect Cargo including WMD (UNCLAS Annex)
- (TSI6) Suspect Crewmen or Employee (UNCLAS Annex)
- (TSI7) Explosion in Port (UNCLAS Annex)
- (TSI8) Large-scale Illegal Demonstration (UNCLAS Annex)
- (TSI9) Port Mass Evacuation (UNCLAS Annex)

## 5330 (U) Linkage with applicable Federal, State, Port, & Local plans

Homeland Security Presidential Directive Five (HSPD-5) eliminated the distinction between consequence management and crisis management, and this policy directive has been further defined in the National Response Plan. A security incident by its very nature, however, contains emergency safety, security, and environmental response/recovery concerns. Some of these elements have been well worked out in existing federal, state, port, and local plans; the purposes of the TSIRPs listed in section

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-4
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



5320 is not replace these existing environmental response, public health, and emergency services plans, but rather to network them together with the security plans in the TSIRPs. Accordingly, many if not all of the TSIRPs in section 5320 will active various and sundry existing plans, and those linkages are outlined in section 1700 of this plan.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-5
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 5400 (U) Maritime Security Exercise Requirements

The recommended methodology for building an effective exercise program is to utilize a Talk, Crawl, Walk and Run progressive training system.

**Talk:** This is the stage for scheduled and regular AMS Committee meetings to discuss various scenarios and review duties and responsibilities for each of the critical decision makers. This will afford an opportunity to eliminate unfamiliar terminology and miscommunications. (Planning)

**Crawl:** At this stage a telephonic alert to test the emergency contact system may be used. Other primary and alternate methods of contact should also be tested. It is recommended that this phase be tested at different times to find out where there may be contact problems during certain periods. To find the most reliable method, several methods of contact should be attempted and then incorporated into the primary means. (Notifications)

**Walk:** This form of exercise should be an announced exercise that tests the ability of the crisis operations committee to form and perform their initial stages of crisis response planning. Effective area analysis should be performed to find out when and where potential traffic and other routine activities may interfere with the crisis response committee. (TTX)

**Run:** This is a full dress rehearsal that will involve multi-agency and multi-echelon crisis response elements that range from 1st responder all the way thru 3rd responders. This should be advertised so as to not cause public alarm. It is recommended to conduct one type of scenario, perform an after action review, and then conduct several others if permitted in order to afford the best use of these resources while brought together. (FTX & TTX)

In order for these exercises to be successful they should be as realistic as possible. It is understood that many key players have to sacrifice time and money in order to participate. If at all possible the community should be involved to the fullest extent.

## 5410 (U) Purpose of Exercise Program

The AMS Plan shall be exercised periodically to test the currency and efficiency of the plan's contents. Exercises may include notification, tabletop, or full-field exercises.

The purpose of an AMS exercise is to validate risk mitigation strategies developed during the planning process and identified in the AMS Plan.

The exercise program shall focus on risk reduction methodology and will be designed to determine the validity of the measure. The exercise program shall become a part of the AMS planning process and will serve as a measurement tool to assess and improve risk reduction methods identified in the security plan. Exercise design will be based on threat information and include setting MARSEC Levels.

The designed exercise may be tabletop, field, or a combination of both types. The exercise program shall be attentive to identifying elements of the AMS Plan and AMS Committee process that should be improved. Results of the exercise program are expected to help update and improve the AMS Committee coordination, close gaps within the AMS Plan and improve the security of the maritime domain.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-6
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

The Port Security Committee is **required** to accomplish an exercise once a year with no more than 18 months between exercises. The Committees have developed a 5-year exercise program that details and prioritizes AMS Plan strategies to be analyzed.

## 5420 (U) Goals of the AMS Exercise Program

AMS exercises should be viewed as an opportunity for plan holders to make continuous improvements to their response plans and to their response system. Plan holders can use issues that arise during the evaluation of the exercise to make necessary changes to their response plans to maintain the highest level of preparedness.

The following goals of the Exercise Program shall be kept in mind when developing exercise scenarios:

- Determine the performance-based components of the mitigating strategy;
- Gauge the effectiveness of enhanced security measures at critical operations within the port area.
- Create a pool of enhanced adversary characteristics and lessons learned;
- Establish interaction protocols with other Federal, State and local law enforcement agencies likely to be involved in the overall protection of MTS.
- Update the exercise-planning guideline.

The exercise protocols are designed to give a performance-based appraisal of risk mitigation strategies within a given area.

## 5430 (U) Exercise Cycle

The Port Security Committee is **required** to accomplish an exercise once a year with no more than 18 months between exercises. The Committees have developed a 5-year exercise program that details and prioritizes AMS Plan strategies to be analyzed. All funding for exercises will be provided for by each participating Committee Member for their own equipment, personnel and time. The Port Security Committee Exercises Sub-committee is charged under this plan with serving as the Exercise Design Team and creating the Concept of Exercise.

<u>Date</u>	<u>Type</u>	<u>Name/Scenario</u>
Summer 2004	FTX	<b>BASTION '04.</b> Full-scale test of full MJTF activation under the National Incident Management System, MARSEC TWO communication and attainment following an initiating Transportation Security Incident in the Port of Jacksonville. Jointly assigned to the JMTX Port Security Committee Exercise Subcommittee, the Port Canaveral Security Committee Exercise Subcommittee, and both MJTFs.
Winter 2005	FTX	<b>PALISADE '05.</b> Anticipated creditation for surge deployment around Superbowl XXXIX in Jacksonville during January/February 2005. Assigned to the JMTX Port Security Committee Marine Event Subcommittee.
Summer 2006	CP	<b>SCARP '06.</b> Test of MJTF's ability to activate a Unified Command Post under the National Incident Command System in the Port Canaveral Region. Assigned to the Port Canaveral Security Committee Exercise Subcommittee and MTJF.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-7
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Summer 2007	TTX	<b>RAMPART '07.</b> Test of the links between the Area Contingency Plan, Comprehensive Emergency Management Plans (County), and Area Maritime Security TSI Response Procedures revolving around a suspect/actual disease outbreak in the Jacksonville Region. Assigned to the JMTX Port Security Committee Exercise Subcommittee and MJTF.
Summer 2008	FTX	<b>RAVELIN '08.</b> Full-scale test of September 11, 2001, type incident including emergency shift from MARSEC ONE to MARSEC THREE including full MJTF Activation under the NIMS, MARSEC THREE communications and attainment, particular focus on Operational Security Measures. Jointly assigned to the JMTX Port Security Committee Exercise Subcommittee, the Port Canaveral Security Committee Exercise Subcommittee, and both MJTFs.

## 5440 (U) Scheduling and Design

The detailed exercise schedule shall be developed by the exercise subcommittees to reflect the planning cycle so that information garnered during this process can affect upcoming revisions to the AMS Plan.

A joint design team develops AMS exercises. The joint design team is comprised of representatives from the federal, state, and local government, as well as industry players. The lead plan holder (the organization which holds the primary plan to be exercised) will take the lead on the joint design team, and have the final word on designing the scope of the exercise scenario.

The following shall be included in designing the exercise program:

- Objectives – Develop exercise goals.
- Concept Development – How will the objectives be attained?
- Scenario and Strategy Selection – Determine the correct strategy and scenario selection to meet exercise objectives.
- Conduct of Exercise – Define how the exercise will meet design objectives and detail scope.
- Control and Evaluation – Detail evaluation and control protocols.
- Data Collection – How will the data be fused?
- After-Action Report – The report will include all aspects of the evaluation process and detail corrective action.
- Corrective-Action Plan – How will the corrective action be undertaken? Detail the methods used to implement change.
- Typically involve 1 or more industry players;
- Involve some level of equipment deployment;
- Encourage exercise play in normal operational spaces;
- Stress the dynamics of the decision making process, using NIMS;
- Emphasize the formation of a Unified Command; and, Use NIMS.
- Can vary in length from 8-12 hours to several days in duration.

Exercises offer a wide range of flexibility on incident types, and actual length of exercise play. There are four basic types of exercise lengths that are offered:

- 8-12 hour real time exercise – This type of exercise focuses on the formation of the Unified

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-8
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

Command and the initial response activities, which occur in the early hours of the response evolution.

- 2 day split (8-12 hours each day) – This type of exercise is used to look at the formation of the Unified Command, while also looking at the support elements. This type of exercise simulates play during the evening hours. There are two advantages to this type of exercise. First it allows the players to take a break and rest during the evening hours, and secondly it allows players the opportunity to take a "time-out" in play to reflect on their actions taken up to the end of play at the end of day 1.
- 2 day(Table -top exercise and real time exercise)- Day 1 of this exercise is a table top exercise for the primary members of the Spill Management Team. Day 2 is the complete formation of the Incident Command System (ICS) for all responders.
- 12-36 hour real time exercise – This type of exercise focuses on the same issues mentioned above, but also allows players the opportunity to effect shift changes. This type of exercise may be of any length, but will not exceed 36 hours.

## 5450 (U) Consideration of Equivalent Response

When a response to a given threat includes using AMS Plan strategies, the AMS Committee may request credit for completion of an annual regulatory requirement. The District Commander giving the credit will ensure that adequate strategy validation and process improvement information has been generated to improve the AMS plan.

Credit may be requested for participation in other Federal, State, municipal, or private sector exercise programs. To receive credit the exercise must implement AMS Plan strategies.

## 5460 (U) Recordkeeping

Exercise documentation must be retained by the Federal Maritime Security Coordinator for 2 years. The Port Security Committee Secretary shall ensure that all exercise documentation that is required to be marked SSI is properly documented and protected from release to the general public.

### The Evaluation of an AMS exercise:

A joint evaluation team evaluates AMS exercises. This joint team meets after the exercise and is comprised of one representative from the federal, state, and local governments and industry. Typically the same members who made the joint design team return to serve on the joint evaluation team. AMS exercises are evaluated to provide:

- Feedback to the plan holders, recommending improvements;
- Improve effectiveness of the plan holder in a non-threatening environment;
- Recommend improvements for the training of personnel; and,
- Lessons learned, to be shared by the entire nation.
- Corrective Action Plan

After the joint evaluation team completes the evaluation report, the report is forwarded to the lead federal plan holder for approval and dissemination to the appropriate federal, state, and local governments and industry participants.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-9
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.

## 5470 (U) Linkages between Family of Plans within the Area

Area Maritime Security Exercises shall be designed to test the linkages between Maritime Security Plans (Vessel Security Plans, Facility Security Plans, and Area Maritime Security Plans) in addition to testing the Area Maritime Security Plan itself. Accordingly, Area Exercises may initiate as a cascade up (an incident at a facility or vessel which includes activation of the Area Maritime Security Plan as spelled out in each vessel or facility security plan), or cascade down (an incident at the national, regional, or area level that requires activation of facility and vessel security plans as in a MARSEC level change).

These links within the family of plans are key to the success of the Maritime Security system as a whole, and must be routinely exercised. Within a given five year time frame, both cascade up and cascade down linkages should be exercised.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	5000-10
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the paragraphs containing SSI are removed.



## 6000 CONSEQUENCE MANAGEMENT AND RECOVERY

This section details how the consequences of a terrorist attack will be managed and how emergency recovery efforts will be coordinated. This section is organized as follows:

- 6100 Introduction
- 6200 Procedures to Maintain MTS
  - 6210 Major Transportation Routes
    - 6211 Bridges
    - 6212 Waterways
  - 6220 Military Critical Shipping Channels
  - 6230 Military Critical Port Areas
  - 6240 Secondary Transportation Routes
    - 6241 Bridges
    - 6242 Waterways
  - 6250 Commercially Critical Shipping Channels
  - 6260 Commercially Critical Port Areas
  - 6270 Public/Recreational Waterways
- 6300 Procedures for Recovery of MTS
  - 6310 Major Transportation Routes
    - 6311 Bridges
    - 6312 Waterways
  - 6320 Military Critical Shipping Channels
  - 6330 Military Critical Port Areas
  - 6340 Secondary Transportation Routes
    - 6341 Bridges
    - 6342 Waterways
  - 6350 Commercially Critical Shipping Channels
  - 6360 Commercially Critical Port Areas
  - 6370 Public/Recreational Waterways

### 6100 (U) Introduction

Normally, non-emergency post-incident recovery of the Marine Transportation System after a Transportation Security Incident will be coordinated through the Federal Maritime Security Coordinator and government agencies, along with the private sector.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	6000-1
-----------------	----------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed.

Specific priorities have been outlined in the AMSA:

- Major transportation routes needed for emergency services or evacuation tunnels, bridges, key waterways.
- Main shipping channels critical for homeland security and homeland defense operations.
- Port areas and channels critical for military traffic or outloads.
- Secondary bridges, tunnels.
- Main shipping channels critical to major commercial operations.
- Secondary commercial waterways.
- Public/recreational waterways.

## 6200 (U) Procedures to Maintain MTS

The procedures outlined in this section differ from the procedures for protecting critical infrastructure in a pre-incident environment. Following an incident, not only do the risk scores skyrocket due to the actual incident but the value of the remaining infrastructure increase proportionally as well. It is important to note that recent events and intelligence information indicate an increased practice of using multiple simultaneous attacks to the increase the likely of success, cause the greatest amount of casualties and disruption to the target. Throughout this section it is assumed that single attack is likely to be followed another. Though the immediate focus will be to respond to the site of the initial incident it is equally if not more important to focus on eliminating opportunities for subsequent incidents to take place.

## 6210 (SSI) Major Transportation Routes

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 6211 (SSI) Attack on Bridge

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 6212 (SSI) Waterway Obstruction (Vessel Sinking)

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	6000-2
-----------------	----------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed.

## 6220 (SSI) Military Critical Shipping Channels

[Reserved]

## 6230 (SSI) Military Critical Port Areas

[Reserved]

## 6240 (SSI) Secondary Transportation Routes

[Reserved]

## 6250 (SSI) Commercially Critical Shipping Channel

[Reserved]

## 6260 (SSI) Attack on a Shoreside Facility

[Reserved]

## 6270 (SSI) Vessel Explosion in Recreational Waterway

[The Federal Maritime Security Coordinator has redacted this information from this version of the Area Maritime Security Plan. If you are a “covered person” under 49 CFR part 1520 with a need to know this information, contact the Federal Maritime Security Coordinator for information about how to receive Sensitive Security Information. See also section 3500 of this plan.]

## 6300 (SSI) Procedures for Recovery of MTS

[Reserved]

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	6000-3
-----------------	----------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520. The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed.

## 7000 COMPLIANCE MEASURES

This section is organized as follows:

- 7100 [Introduction](#)
- 7200 [Reserved](#)

### 7100 Introduction

The MTSA regulations rely on existing COTP authority if compliance measures need to be taken. Operational controls are normally exercised as a preventative measure when it is necessary to secure nonconforming vessels or facilities to adequately reduce or prevent risks of a TSI, injury or damage to vessels or facilities.

The control and compliance measures contained in [33 CFR 101.410](#) provide the COTP with a large degree of flexibility to assure appropriately low security risk of both vessels and facilities operating within the zone. Guidance on using controlling measures is contained in [the Marine Safety Manual \(MSM\), Volume I, Chapter 4](#) and will be considered when taking such action. In some cases, a violation may carry both potential civil and criminal penalties. In cases where evidence exists that a major violation has occurred, the matter should be referred to the District Commander in accordance with MSM Vol. I, 4.D.2.d.

#### 33CFR 101.410

- (a) The COTP may exercise authority pursuant to 33 CFR parts 6, 160 and 165, as appropriate, to rectify non-compliance with this subchapter. COTPs or their designees are the officers duly authorized to exercise control and compliance measures under SOLAS Chapter XI-2, Regulation 9, and the ISPS Code (Incorporated by reference, see §101.115).
- (b) Control and compliance measures for vessels not in compliance with this subchapter may include, but are not limited to, one or more of the following:
  - (1) Inspection of the vessel;
  - (2) Delay of the vessel;
  - (3) Detention of the vessel;
  - (4) Restriction of vessel operations;
  - (5) Denial of port entry;
  - (6) Expulsion from port;
  - (7) Lesser administrative and corrective measures; or
  - (8) Suspension or revocation of a security plan approved by the U.S., thereby making that vessel ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).
- (c) Control and compliance measures for facilities not in compliance with this subchapter may include, but are not limited to, one or more of the following:
  - (1) Restrictions on facility access;
  - (2) Conditions on facility operations;
  - (3) Suspension of facility operations;
  - (4) Lesser administrative and corrective measures; or
  - (5) Suspension or revocation of security plan approval, thereby making that facility ineligible to operate in, on, under or adjacent to waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).
- (d) Control and compliance measures under this section may be imposed on a vessel when it has called on a facility or at a port that does not maintain adequate security measures to ensure that the level of security to be achieved by this subchapter has not been compromised.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	7000-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

# 7200 Reserved

This section is reserved for future development.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	7000-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

## 8000 PLAN DOCUMENTATION AND MAINTENANCE

This series outlines the processes by which this plan has been created, reviewed, commented upon, and approved, and the procedures by which both the Area Maritime Security Assessment and Area Maritime Security Plan will be updated annually along with audits of the plan as implemented. This series is organized as follows:

- 8100 Initial Plan Review and Comment
- 8110 Procedures For Continuous Review And Update Of AMS Plans
  - 8110.1 Annual Informal Review
  - 8110.2 Procedures to Formally Update AMS Plan
  - 8110.3 Perishable Information Management
  - 8110.4 Submission of Updates
- 8120 Procedures for Continuous Review and Update of the AMS Assessment

### 8100 Initial Plan Review and Comment

In accordance with Title 33 part 103 and Coast Guard policy, the Federal Maritime Security Coordinator consulted with the JMTX Port Security Committee and the Port Canaveral Security Committee regarding the initial draft of this plan, then (after taking into account the input received), submitted the AMS Plan to the Commander, Seventh Coast Guard District for review. The FMSC submitted the plan both electronically on CD Rom and in paper.

The Commander, Seventh Coast Guard District reviewed the initial draft AMS Plan for completeness, and then forwarded it to the Coast Guard Commander, Atlantic Area, who is the approval authority. Upon approval, Commander, Atlantic Area forwarded an electronic version of the (now) approved AMS Plan to the Commandant (G-MP) of the Coast Guard.

Key dates in this initial plan review and comment process were:

Date	Event
03 December 2003	Executive Subcommittees of the JMTX Port Security Committee and Port Canaveral Security Committee met in closed session to provide comments on both the UNCLAS and SSI Security Measures and OPSEC Measures to be contained in the plan. Specific comments are documented in the minutes of the Executive Subcommittee meeting. Changes to the security measures and OPSEC measures were integrated into the full Area Maritime Security Plan.
19 December 2003	The FMSC made the first draft of the full Area Maritime Security Plan available for port-wide comments. The FMSC redacted SSI sections from the public version, and made the full plan available to members of the Executive Subcommittees. All final comments were to be submitted by e-mail to the FMSC not later than Friday, 16 January 2004.
16 January 2004	Comment period on the plan closed.
15 March 2004	The FMSC forwarded this plan to the Commander, Seventh Coast Guard District for review.
01 July 2004	This plan was approved by the Commander, Atlantic Area and returned for implementation to the Federal Maritime Security Coordinator. See the letter of distribution in the 1000 series.

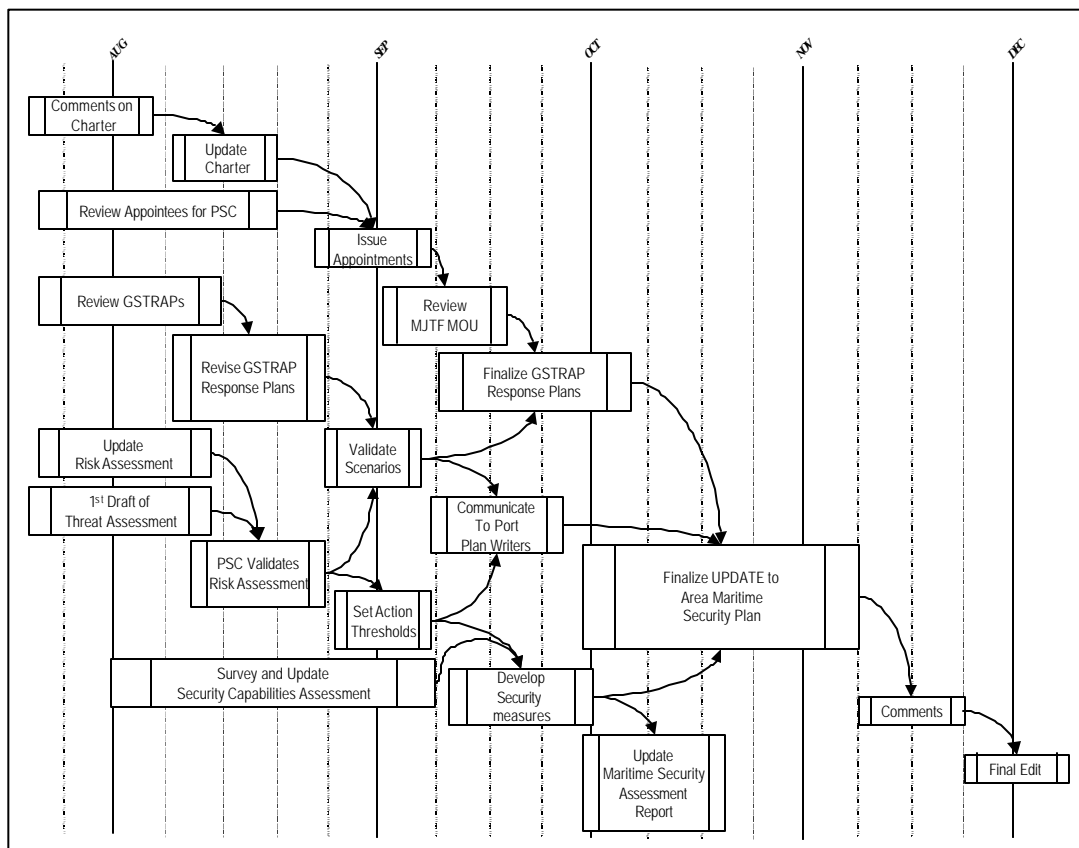
VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	8000-1
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

## 8110 Procedures For Continuous Review And Update of AMS Plans

This section outlines the procedures the Port Security Committee will use to continuously review and update the AMS Plan.

### 8110.1 Annual Informal Review

At least once each year, the FMSC will conduct an informal review and update of the AMS Plan for adequacy, feasibility, consistency and completeness and to identify gaps in security. The FMSC will use the following process to accomplish the annual informal reviews:



The update and review of the AMS Plan is an ongoing process. The FMSC, in coordination with the Port Security Committees, will review the activated portions of the AMS Plan after each activation, exercise, or drill, and when port conditions change. After each review, the plan will be updated to include any lessons learned from the activation exercise or drill, and reflect any changed port conditions. The Port Security Committee's Exercises Subcommittee will assure that technical update of the AMS Plan is integrated into the Concept of Exercise, and the Demobilization Plan for any incident response must include hot-wash and technical update of the AMS Plan as part of the Incident Action Plan.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	8000-2
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------



## 8110.2 Formal Review

Under 33 CFR part 103 and Coast Guard policy, the FMSC must conduct a formal review of the AMS Plan every five years. As part of these reviews, the FMSC will consult with the JMTX Port Security Committee and Port Canaveral Security Committee to review and update the AMS Assessment and Plan incorporating changes in the port operations and infrastructure.

## 8110.3 Perishable Information Maintenance

Portions of the AMS Plan must be immediately updated when certain critical items of information change including:

- Emergency points of contact by name and number.
- SSI eligible recipients with their pertinent verification data.
- Any changes that alter the communications or notification plan.
- Any changes in jurisdictional or response capabilities.
- Any major or minor construction changes that alter avenues of access to facilities.

## 8110.4 Submission of Updates

The FMSC will submit updates of the AMS Plan to the Commander, Seventh Coast Guard District and Commander, Atlantic Area as appropriate for review and approval annually, or as substantive changes are made. To facilitate auditing, the FMSC and Port Security Committees will maintain a record of changes and lessons learned when reviewing and updating the AMS Plan for reasons described in section 8300 of this Plan.

## 8120 Procedures for Continuous Review and Update of the AMS Assessment

The FMSC will annually audit the AMS Assessment to ensure that material contained in the assessment is up to date and the threat processes, initiatives, and restrictions are accurate and effective.

The AMS assessment will also be reviewed and updated to incorporate changes in the port operations and infrastructure. Like the AMS Plan Update and Review, conducting routine maritime security assessments is an ongoing process. Accordingly, the assessment should be informally evaluated at least annually for adequacy, feasibility, consistency, completeness and to identify gaps in security.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLASSIFIED	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	8000-3
-----------------	--------------------	---------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

## 9000 APPENDICES

This plan contains many appendices with detailed information which, if presented in the plan itself, would unduly interrupt the flow of the plan or make the plan more difficult to understand and use. The following appendices are referenced in the plan:

- 9100 [Elements of Maritime Homeland Security](#)
- 9200 [Port Security Committee Executive Subcommittee Members](#)
- 9300 [Charts and Maps of Port Areas](#)
- 9400 [AMS Assessment](#)
- 9500 [Communications Plan](#)
  - TAB A: [Standard MJTF Communications Plan](#) (SSI)
  - TAB B: Communications with Commercial Vessels
  - TAB C: Communications with Facilities
  - TAB D: Communications with Companies
  - TAB E: Communications with Marinas
  - TAB F: Communications with SSI-Eligible Persons
  - TAB G: Communications with Waterway Users (Boaters)
  - TAB H: MSIB to set MARSEC TWO
  - TAB I: MSIB to step down to MARSEC ONE
  - TAB J: MSIB to go from MARSEC ONE to MARSEC THREE
  - TAB K: MSIB to go from MARSEC TWO to MARSEC THREE
  - TAB L: MSIB to go from MARSEC THREE to MARSEC TWO
  - TAB M: BNTM to set MARSEC ONE
  - TAB N: BNTM to set MARSEC TWO
  - TAB O: BNTM to set MARSEC THREE
  - TAB P: MJTF Notifications
  - TAB Q: MARSEC Communication E-Mail Template
- 9600 Security Incident Response Procedures
  - TAB A: Suspicious Activity Response Procedures
    - SA-1: Bomb Threats ([UNCLAS](#)) ([SSI](#))
    - SA-2: Access Attempt ([UNCLAS](#)) ([SSI](#))
    - SA-3: Photo Surveillance ([UNCLAS](#)) ([SSI](#))
  - TAB B: Security Breach Response Procedures
    - SB-1: Trespass, Stowaway, or Boat in Security Zone ([UNCLAS](#)) ([SSI](#))
    - SB-2: Small-scale Illegal Demonstration ([UNCLAS](#)) ([SSI](#))
    - SB-3: Security System Tampering (UNCLAS) (SSI)
    - SB-4: Security Measure Not In Place (UNCLAS) (SSI)
  - TAB C: Transportation Security Incident Response Procedures
    - TSI-1: Rogue Vessel (UNCLAS) (SSI)
    - TSI-2: Possible Bioterrorism (UNCLAS) (SSI)
    - TSI-3: Explosive Device Discovery (UNCLAS) (SSI)
    - TSI-4: Intrusion w/ Small Arms (UNCLAS) (SSI)
    - TSI-5: Suspect Cargo including WMD (UNCLAS) (SSI)
    - TSI-6: Suspect Crewmen or Employee (UNCLAS) (SSI)
    - TSI-7: Explosion (UNCLAS) (SSI)
    - TSI-8: Large-Scale Illegal Demonstration (UNCLAS) (SSI)
    - TSI-9: Evacuation of the port (UNCLAS) (SSI)
  - TAB D: Geographically-Specific Transportation Security Incident Response Procedures

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9000-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

[RESERVED]

- 9700 MJTF Incident Action Templates  
TAB A: MARSEC ONE (SSI)  
TAB B: MARSEC TWO (SSI)  
TAB C: MARSEC THREE (SSI)  
TAB D: Military Outload (SSI)  
TAB E Major Marine Event (SSI)
- 9800 [Glossary of Terms](#)
- 9900 Interagency Agreements  
9910 [Sign Port Security Committee Charter](#)  
9920 [Maritime Joint Task Force](#)  
9930 [Port Facilities Form Details](#) (SSI)  
9940 Public Access Facilities  
TAB A: Public Access Facility Exemption Request Template  
TAB B: Standard and Additional PAF Security Measures (SSI)  
TAB C: PAF Designations and Acknowledgement Letters [reserved]  
TAB D: Publicly Available List of PAFs [reserved]
- 10000 Dangerous Cargoes for Security Planning  
10010 Introduction  
10011 Implications of Dangerous Cargoes in Security Planning  
10012 Scenario Based Planning  
10012.1 Hazard Analysis and Inventory  
10020 Database of Dangerous Cargoes

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9000-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

## Appendix 9100 Elements of Maritime Homeland Security

The term “terrorism” is defined as “the calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.” This definition is the foundation throughout this plan for the doctrine and guidance to vessel operators, facility operators, critical infrastructure owners and operators, and the Maritime Joint Task Force. This appendix is organized as follows:

- 9110 [Elements of PWCS](#)
  - 9111 [Anti-terrorism](#)
  - 9112 [Counter-terrorism](#)
  - 9113 [Response to Terrorism](#)
  - 9114 [Consequence Management following Terrorism](#)
- 9120 [Terrorism](#)
  - 9121 [Terrorist Tactics](#)
  - 9122 [Terrorist Groups](#)
  - 9123 [Terrorist Organizations](#)
  - 9124 [Terrorist Targets – Americans](#)
  - 9125 [Domestic Terrorism](#)

### 9110 Elements of PWCS

Ports, Waterways, and Coastal Security (PWCS) involves actions including anti-terrorism (AT) (defensive measures used to reduce the vulnerability to terrorist acts), counter-terrorism (CT) (offensive measures taken to detect, deter, disrupt, and halt to terrorist action), terrorism-response (RT) (emergency actions taken to remove a terrorist attack vector and prevent further loss of life, economic damage, or environmental damage), and terrorism consequence management (CMT) (non-emergency actions taken to restore vital services and functions on an interim basis until permanently restored), taken to oppose terrorism throughout the entire threat spectrum. This plan addresses all four elements of PWCS. The following definitions are provided to assist in understanding the difference between AT, CT, RT, and CMT:

#### 9111 Anti-terrorism

Anti-terrorism is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local security forces.

#### 9112 Counter-terrorism

Counter-terrorism is offensive measures taken to detect, deter, disrupt, and halt ongoing terrorism. Sensitive and compartmented CT programs are addressed in relevant Homeland and National Security Decision Directives, National Security Directives, contingency plans, and other relevant classified documents.

#### 9113 Response to terrorism

Response to Terrorism (RT) is emergency action taken to remove a terrorist attack vector and (by doing so) prevent further loss of life, economic damage, or environmental pollution. Typically, RT includes crisis management, mass casualty rescue and environmental pollutant response (including public health vectors).

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

## 9114 Consequence Management after Terrorism

Consequence Management for Terrorism (CMT) is non-emergency action taken to restore vital maritime and civic services and functions on an interim basis until permanently restored. CMT activities may include temporary provision of transportation services, public order law enforcement, food and water distribution, communications services, harbor/river dredging, and salvage operations.

## 9120 Terrorism

This section has been adapted from Department of Defense Joint Pub 3.07-2 (JTTP for Antiterrorism, dated 17 March 1998). A critical factor in understanding terrorism is **the importance of the emotional impact of the terrorist act on an audience other than the victim**. This chapter provides background information concerning the terrorist threat to enable security officers to create and employ homeland security tactics, techniques, and procedures outlined in this pub. Terrorism has become a media event and, as such, a phenomenon of our time. The terrorist of today will exploit information operations against the United States as much as the media will allow. News media coverage is important to terrorists who are attempting to incident public fear or gain attention for their cause. Another determinant of tactics and target selection is the role the terrorist group perceives itself as playing. Terrorism can also be used as either an overt or a covert aspect of a political struggle within an existing political system. Terrorists frequently claim affiliation with causes or political organizations to give their actions a claim of respectability. Operations to meet the threat may fall in any of the four PWCS categories: anti-terrorism, counter-terrorism, terrorism response, or terrorism consequence management.

## 9121 Terrorist Tactics

Terrorist tactics vary in sophistication according to the level of training the individual or group has received. Categories of training are: trained (the entire group has had formal training); semi-trained (a few members have been trained and have passed that training on to the rest of the group); and untrained (no members have had formal training). Just as a terrorist incident may have several objectives, the tactics used may also be combined. The more common tactics employed by contemporary terrorists are discussed below.

**ASSASSINATION.** A term generally applied to the killing of prominent persons and symbolic enemies as well as traitors who defect from the group.

**ARSON.** Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only a low level of technical knowledge.

**BOMBING. The improvised explosive device (IED) is the terrorist's weapon of choice.** IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. (However, suicidal bombing cannot be overlooked as an employment method.) Other advantages include their attention-getting capacity and the ability to control casualties through time of detonation and placement of the device. It is also easily deniable should the action produce undesirable results. From 1983 through 1996, approximately half of all recorded terrorist incidents involved IEDs. In general aircraft are the preferred target because of their greater mobility and vulnerability. Events during 2002 have demonstrated the willingness, ease, and ability to use **small boats as IED transportation devices (like a car-bombing or suicide attack) against large naval and economic vessel targets**. Logically, these tactics can also be used against port installations and critical infrastructure.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

**HOSTAGE TAKING.** This usually is an overt seizure of one or more individuals with the intent of gaining publicity or other concessions in return for release of the hostage. While dramatic, hostage and hostage barricade situations are risky for the perpetrator.

**KIDNAPPING.** While similar to hostage taking, kidnapping has significant differences. **Kidnapping is usually a covert seizure of one or more specific persons in order to extract specific demands.** The perpetrators of the action may not be known for a long time. News media attention is initially intense but decreases over time. Because of the time involved, successful kidnapping requires elaborate planning and logistics. The risk to the terrorist is less than in the hostage situation.

**HIJACKING OR SKYJACKING.** Sometimes employed as a means for escape, **hijacking has in the past been carried out to produce a spectacular hostage situation.** Although trains, buses, and ships have been hijacked, aircraft are the preferred target because of their greater mobility and vulnerability. Following the events of September 11<sup>th</sup>, 2001, however, we can no longer assume that hijackings of major transportation means (larger aircraft, ships, etc.) are simply hostage taking. In fact, **transportation can be used as a major vector for attack where the vessel or aircraft itself becomes the weapon.** Given our awareness of this tactic, it is likely that terrorists will try to mislead responders by claiming a hostage-taking (instead of a rogue-vessel / rogue aircraft attack) during future hijacking events.

**ROGUE VESSELS OR AIRCRAFT.** Sometimes employed as a means for escape, fund raising/money laundering, logistical supply, or infiltration, terrorist organizations have purchased and operated aircraft and merchant vessels disguised as legitimate transportation traffic. Although these international means of transportation have not (to date) been used as an attack vector, they can be used to transport IEDs or larger non-conventional weapons of mass disruption / destruction. Such tactics require continuous vigilance of our airspace and maritime approaches because rogue vessels and aircraft can “appear” without making advance notice typical to legitimate neutral (white) shipping. The challenge is distinguishing rogue (red) shipping from white shipping.

**ROGUE CARGO.** Typically employed to transport money, logistical supplies, or to infiltrate, terrorist organizations have used the enormous flow of commercial cargo (by ship, air, rail, and truck) by disguising their actual cargo as innocuous general cargo (optimally in sealed shipping containers). As with rogue vessels or aircraft, these tactics have not yet been used as a direct attack vector, but **they can be used to transport IEDs or larger non-conventional weapons of mass disruption / destruction (in particular dirty bombs or improvised nuclear devices).** The enormous volume of neutral (white) cargo makes screening extremely difficult.

**SEIZURE.** Seizure usually involves a building or object that has value in the eyes of the audience. There is some risk to the terrorist because security forces have time to react and may opt to use force to resolve the incident, especially if few or no innocent lives are involved.

**RAIDS OR ATTACKS ON FACILITIES.** Armed attacks on facilities are usually undertaken for one of three purposes: to gain access to radio or television broadcast capabilities in order to make a statement; to demonstrate the government’s inability to secure critical facilities or national symbols; or to acquire resources (e.g., robbery of a bank or armory).

**SABOTAGE** The objective in most sabotage incidents is to **demonstrate how vulnerable society is to terrorist actions.** Industrialized societies are more vulnerable to sabotage than less highly developed societies. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and gains immediate public attention. Sabotage of industrial or commercial facilities is one means of identifying the target while making a statement of future intent.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-3
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

Facilities and military installations, information systems, and information infrastructures may become targets of terrorist sabotage.

**HOAXES.** Any terrorist group that has established credibility can employ a hoax with considerable success. A threat against a person's life causes that person and those associated with that individual to devote time and effort to security measures. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. False alarms dull the analytical and operational efficiency of key security personnel, thus degrading readiness.

**USE OF SPECIAL WEAPONS.** Chemical weapons have been used by terrorists and there is potential for the use of both chemical and biological weapons in the future. These types of weapons, relatively cheap and easy to make, could be used in place of conventional explosives in many situations.

**The potential for mass destruction and the deep-seated fear most people have of chemical and biological weapons could be attractive to a group wishing to make the world take notice.** Although an explosive nuclear device is acknowledged to be beyond the reach of most terrorist groups, a chemical or biological weapon or a radiological dispersion device using nuclear contaminants is not. The technology is simple and the cost per casualty (for biological weapons in particular) is extremely low — much lower than for conventional or nuclear explosives. This situation could change as the competition for headlines increases.

**ENVIRONMENTAL DESTRUCTION.** Although this tactic has not been widely used, the increasing accessibility of sophisticated weapons and explosives to terrorists has the potential to threaten damage to the environment. Examples would be intentional dumping of hazardous chemicals into a city's water supply or the destruction of an oil tanker.

**USE OF TECHNOLOGY.** Technology has important implications for the terrorist threat. Infrastructure technologies provide attractive targets for terrorists who can apply a range of rudimentary and advanced attack techniques to disrupt or undermine confidence in a range of systems. Key elements of the national infrastructure, such as transportation, telecommunications, energy, banking, public health, and water supply are becoming increasingly dependent on computerized systems and linkages.

- These systems provide targeting opportunities for adversaries who possess even limited technological capabilities, and who have the ability to identify critical system choke points. Terrorists can apply computer generated attacks or more traditional means such as bombs or physical destruction to cause system-wide malfunctions. Interdependencies of systems, such as power and transportation, exacerbate this vulnerability. Significant disruption of power grids can have a devastating impact on air traffic control, railway operations, port operations, and emergency services such as fire and/or rescue and police. Attacks such as power outages also impact a wide segment of the population, command significant media attention and consequently provide an effective means for the terrorist to reach a "captive" audience.
- A range of technologies can also be employed effectively by terrorists to conduct operations. Although terrorists to date have not demonstrated significant technological innovation and have largely relied on traditional attack methods such as bombing, hostage taking, and assaults, several factors point to an increased likelihood of greater use of more sophisticated technologies. First, the wide scale proliferation of military weapons and technologies that has followed the collapse of the former Soviet Union has increased the range of weapons available on international arms markets. Stand-off weapons such as shoulder-fired anti-aircraft weapons, light anti-tank weapons which have been used in attacks against US targets in the past, are attractive means of attack for a terrorist since they reduce vulnerability

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-4
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------



and increase chance of escape. Increased availability of more powerful explosives (such as the plastic explosive Semtex, which is easily concealed and difficult to detect), when combined with more sophisticated timing devices, detonators, and fuses, have provided the terrorist with much more lethal bombing capabilities.

- Increasing availability of nuclear, biological, and chemical (NBC) material, components, and weapons raises the specter of terrorists using these weapons in an attack against civilian populations or military facilities. The 1995 Tokyo subway Sarin nerve gas attack by the Aum Shinrikyo cult, resulting in the death of 12 and injury of 5,500 people, is the most vivid example of the threat from NBC weapons. Many chemical-biological (C-B) weapons ingredients are commercially available, and there are numerous reports throughout Europe of fissile material availability on the black market. This raises the possibility not only of terrorist use of nuclear weapons, but of radiological bombs that use fissile material to contaminate targets.
- A range of commercially available technologies can dramatically enhance terrorist operational capability. These include communications equipment, encryption capabilities, surveillance equipment, weapons, a range of computer and information management technologies, weapons components, and the Internet. The ability to acquire or adapt technologies can give terrorists an edge in choosing targets and conducting attacks as well as significantly expanding their range of attack options.
- Technological advances also enhance antiterrorism capabilities. Recent research and development efforts have focused on the following areas:
  - detection of explosives and other weapons;
  - detection of, and defense against, C-B agents;
  - physical protection (e.g., alarms, barriers, access control);
  - incident response; and
  - data analysis and dissemination.
- Explosive detection technologies can be applied for both airline security and for fixed facilities. They detect physical, chemical, or mechanical properties of bombs using a variety of technologies, from x-rays and radio waves to dogs and “sniffer” technologies.
- Detection of C-B agents poses a significant challenge, since almost anyone that can brew beer can manufacture a biological agent, and toxic chemicals are widely available on the commercial market. Laser technologies have shown promise in detection of C-B agents, and research and development work on personnel protective equipment and vaccines is being pursued aggressively.
- A range of technologies is currently being investigated to enhance physical protection capabilities. Access control technologies, which include a range of personnel identification systems, metal detectors, and closed circuit surveillance devices are being researched and fielded on a regular basis. Barrier technologies are also being fielded, and enhancements in building design to enhance bomb resistance are being incorporated into new and existing DOD buildings in high threat areas.
- Incident response technologies are developed to assist in responding to assaults on facilities, hostage taking, or criminal activities. Incident response activities include disrupting the attack, defending targets, aiding persons injured in an attack, rescuing hostages, and

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-5
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

apprehending attackers. A broad range of technologies are included in this category such as fiber-optic and low-light camera technologies, highly accurate sensors, non-lethal weapons, incapacitating agents, and software tools for profiling terrorists and supporting response planning.

- Effective data dissemination is a key measure to improving antiterrorism awareness and preparedness. The rapid evolution of information technology has facilitated the transfer of accurate terrorist profiles (to include photographs) and the ability to transfer the information anywhere in the world quickly. Other key AT data, such as protection technologies and procedures, can also be transmitted to field locations quickly and effectively. Recent efforts have reduced barriers between agencies on the fusion and dissemination of AT data.

## 9122 Terrorist Groups

A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication. For several years, **security forces categorized terrorist groups according to their operational traditions — national, transnational, and international**. National groups operated within the boundaries of a single nation. Transnational groups operated across international borders. International groups operated in two or more nations and were usually assumed to receive direction and support from a foreign government. **Terrorist groups are categorized by government affiliation** to help security planners anticipate terrorist targets and their sophistication of intelligence and weaponry.

While the three categories broadly indicate the degrees of sophistication that may be expected, it is important to examine each terrorist group on its own terms. The vast funds available to some narco-terrorists afford them the armaments and technology rivaling some nation-states. Messianic religious cults or organizations have features from all three of the listed categories. They may be “nonstate-supported” (e.g., Japan's Aum Shinrikyo cult or the Abdul-Ramman group that perpetrated the World Trade Center bombing), “state-supported” (e.g., extremist factions of HAMAS who believe violence serves their concept of religious servitude), or “state-directed” (e.g., Hizballah is both the “Party of God” and a religious cult organization that employs violence in support of both religion and politics).

## 9123 Terrorist Organization

As with any organization, terrorist groups develop organizational structures that are functional for the environment in which they operate. Because terrorists usually operate a hostile environment, **security is the primary consideration**. As a result, **the organization of terrorist groups is usually cellular, with each cell relatively isolated and performing specific functions such as intelligence gathering or logistic operations**. This type of organization protects members of the group. In the event of defection or capture, no one member can identify more than a few of the others. Some groups have multifunctional cells that combine several skills in one operational entity, while others create cells of specialists that come together for an operation on an ad hoc basis. The latter procedure is similar to tailoring or task organizing military forces.

**SIZE.** Larger terrorist groups (100 or more members) normally have a central command and control element with one or more subordinate elements based on geographical regions. The regional commands direct the actions of the operational and support cells in their region. Smaller groups (50 or fewer members) may have a single command element that directly controls all of the operational and support cells regardless of where they are established.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-6
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

**STRUCTURE.** Terrorist groups often structure themselves in a manner similar to military organizations, but groups vary as to the degree of discipline and lines of authority and function. Such organizations have historically had well-defined, organized structures that made penetration difficult. In other instances, group dynamics, egos, and philosophical differences override organizational principles and create opportunities for security forces to identify members, penetrate the organization, and/or prevent terrorist actions. These **personal factors often cause such terrorist groups to splinter into new faction(s)** (e.g., Popular Front for the Liberation of Palestine, Popular Front for the Liberation of Palestine, and Democratic Front for the Liberation of Palestine), adding to the growing list of organizational titles in world terrorism. Along with the commonly used deception technique of claiming credit for an action in the name of a previously unknown group, **splintering complicates security force intelligence efforts and creates confusion in determining the decision makers**, thus making the organizations generally hard to break. c. In a broader context, **terrorist organizations**, especially those with little or no access to government resources, **need a support structure**. A typical organization consists of operational members who are functionally organized as outlined above and have several categories of supporters.

- **At the top is the leadership** that defines policy and directs action. Typically, leaders are completely committed to the cause that the group purports to serve and may be charismatic figures. If the group is state-supported or state-directed, the leadership will include one or more members who have had extensive training or education by the sponsoring state.
- **The active, operational cadre are the doers** — the men and women who carry out terrorist attacks and train others. As in the planning and leadership elements, many doers are deeply committed to the group's cause. The professionals who may or may not be ideologically motivated are also part of the active cadre.
- **Active supporters do not actually commit violent acts but assist the terrorists by providing money, intelligence, legal or medical services, and/or safe houses or forged documents.** This includes supporters both within the country and in other countries. Active supporters are frequently ideologically in agreement with all or some of the terrorist group's goals but may be ambivalent concerning the use of violence. Terrorist groups recruit most of their cadre from the ranks of the active supporters because those people have proven their loyalty and, to some extent, their skills over a period of time.
- **Passive supporters are the most difficult to define and identify. Most of these people are sympathetic to the terrorist group's cause**, but will not assume an active role due to fear of reprisal if exposed or identified. Family and acquaintances of activists sometimes fall into this category, especially in cultural environments where family and regional loyalties are strong. Often, passive supporters are not sympathetic to the terrorist cause but do not believe that the government can or will protect them. Thus, fear rather than sympathy generates support for the terrorist. Passive supporters may be ignorant to the cause's intent and use of their support; consequently, they may unwittingly provide anonymous funding. The terrorist group relies on passive supporters for financial assistance, displays of public support, and minor logistic or operational tasks. Passive support is extremely important to the politically-motivated terrorist who relies on popular support to survive.

**MEMBERSHIP.** Membership in terrorist organizations brings together people who commit terrorist acts for different motivations. **Not all terrorists are committed to their cause by ideology.** Many terrorist groups are augmented by criminals (professionals) who are opportunists seeking personal rather than political gain or by individuals who are mentally disturbed. **Many individuals responsible for terrorist acts could fit into one of three categories; crusaders, criminals, or emotionally disturbed.**

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-7
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

Although the criminal or emotionally disturbed person may not fit the strict definition of a terrorist, the varied motivations and ambiguities of terrorism necessitate their inclusion in the same context with the crusader. A specific individual may exhibit traits from more than one category. Terrorists look like ordinary citizens and come from all walks of life.

- **Crusaders** are ideologically inspired individuals or groups (e.g., political terrorists). They believe that their cause is so noble or worthy that it may be promoted by any means, including the use of terror.
- **Criminals or professionals** commit terrorist acts for personal gain rather than ideology. Although they often mimic the crusader's ideological conviction, their devotion to the cause is not the primary motivation. Crusaders often recruit criminals for their knowledge, background, and criminal skills.
- **Emotionally or mentally disturbed people** who commit terrorist acts often believe that they have some special mandate from a deity. They can range in character from compulsive, minute planners to impulsive, unpredictable doers. Additionally, emotionally disturbed people often obtain some level of enjoyment in the terrorist act. The emotionally and mentally disturbed are often used by terrorist organizations as throwaway or disposable terrorists. They usually drive the truck bomb or become martyrs for a cause.

## 9124 Terrorist Targets — Americans

It is sometimes difficult for Americans to understand why **terrorism seems to thrive in the environment that offers the least justification for political violence** (e.g., democracies and ineffective authoritarian regimes). Equally puzzling is the relative absence of terrorism in those societies with totalitarian and effective authoritarian governments. The reasons for this apparent paradox can be summarized as being a matter of social control. The terrorist operates covertly. **In societies where little is done without the knowledge of internal security agencies, covert activity for any appreciable period of time is difficult.**

The same principle applies to acquisition of weapons, communications equipment, and explosives. Another factor is public information. Because the terrorist's objectives usually include gaining the attention of a target audience through a violent act, the terrorist can easily be denied that objective in an environment where information media are tightly controlled. Finally, in controlled societies, the ability of terrorist organizations to create functional networks or to move funds within the financial system are severely hindered.

**DIRECT U.S. INTERESTS.** The reasons US interests are a target for so many terrorist groups around the world are complex and must be understood in order to effectively combat terrorism in the long term. **One reason some terrorist groups target the United States and its citizens is ideological differences.** The United States is a leading industrial power and the leading capitalist state. These reasons are enough to incite the animosity of some groups that are committed to different social systems.

**U.S. INFLUENCE.** Of greater importance is the perception that the US Government can dictate courses of action to other governments. Terrorists think that by pressuring the United States through acts of terror, the US Government will bring pressure to bear on the targeted government to comply with terrorists' demands. Although US influence is substantial in the world community, this is not a policy of the US Government.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-8
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

**U.S. PRESENCE OVERSEAS. Mere presence is another factor.** Americans are all over the world in capacities ranging from diplomatic service to tourists. This availability makes targeting Americans easy even for relatively poorly trained non-state-supported groups. It also adds to the chances of Americans being killed or injured unintentionally. These same considerations apply to members of the US military forces with the added factor of “symbolic value.” The Armed Forces and international American Corporations are clearly visible symbols of US projection of power and presence; thus, terrorists find American or related personnel and installations appealing targets.

## 9125 Domestic Terrorism

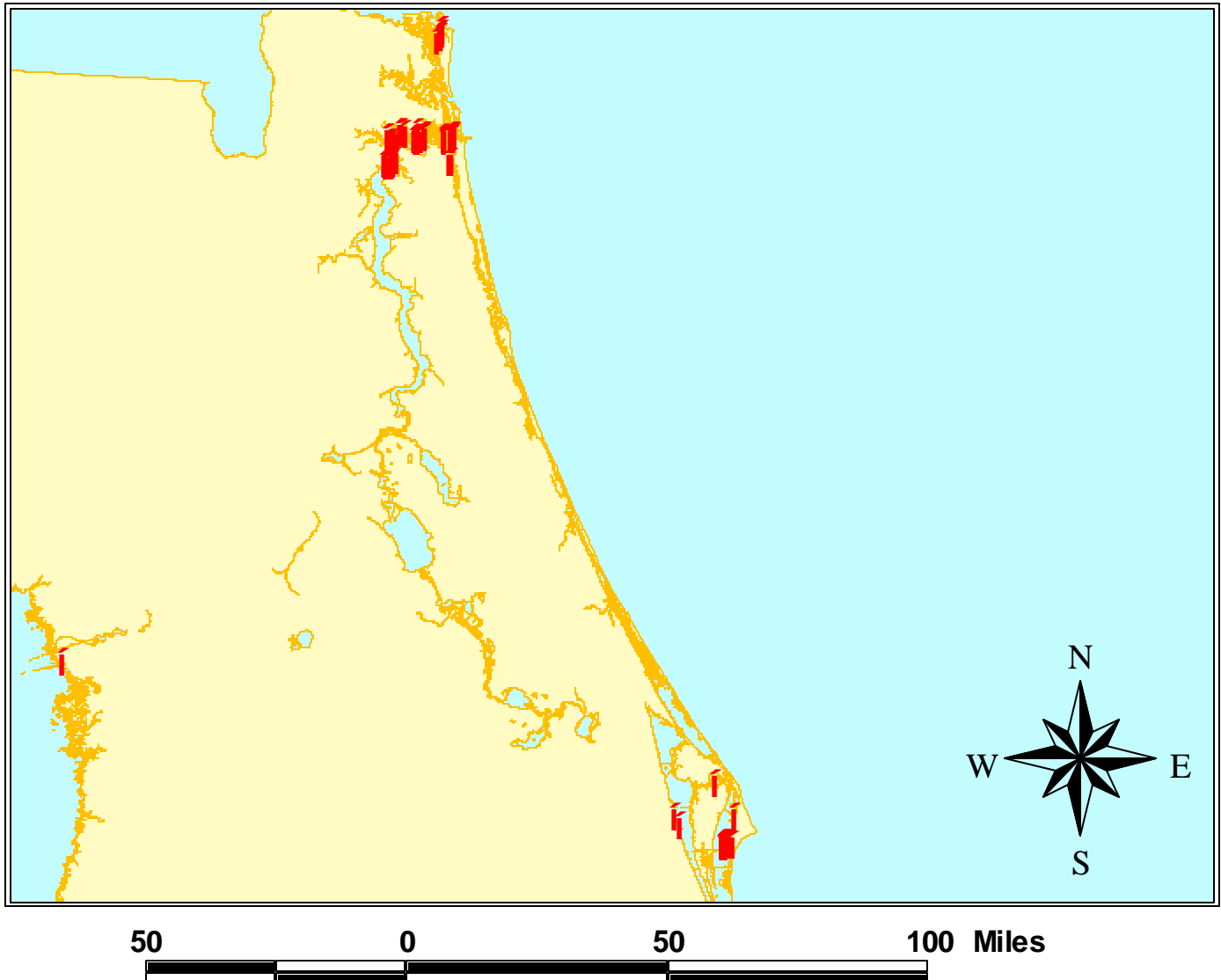
**PAST ATTACKS INSIDE THE U.S.** Despite recent bombings in New York, Oklahoma, and Atlanta, the United States has a low rate of terrorism compared to Europe, Latin America, Africa, or the Middle East. **A tradition of violence for political purposes has not been a dominating means of achieving political power.** There is no history of deep ideological commitment justifying the taking or sacrificing of life. Although there have been limited exceptions to this observation — such as some Puerto Rican independence groups — they have not gained political acceptance at the national level. The relatively open US political system allows minority groups to voice concerns legitimately through the political process.

Recently, however, groups of domestic separatists have targeted federal institutions for violence. These attacks indicate a growing willingness to attack symbols of the US Government, despite the relatively open US political system which allows minority groups to voice concerns legitimately through the political process.

**PREDICTING FUTURE ATTACKS INSIDE THE U.S.** Caution must be exercised in drawing conclusions exclusively from past experiences. Although low levels of domestic terrorism have occurred in the United States to date, terrorism is still a threat here. Radicals and religious extremist organizations and the rise of militias constitute a growing threat to public order. Racial supremacists as well as the violent fringe of environmental and antiabortion movements have also attempted to use terrorism. Agents of external causes and foreign powers pose a potential threat that needs only a transoceanic flight or border crossing to become active. Additionally, computer hackers anywhere in the world can send viruses via the Internet.

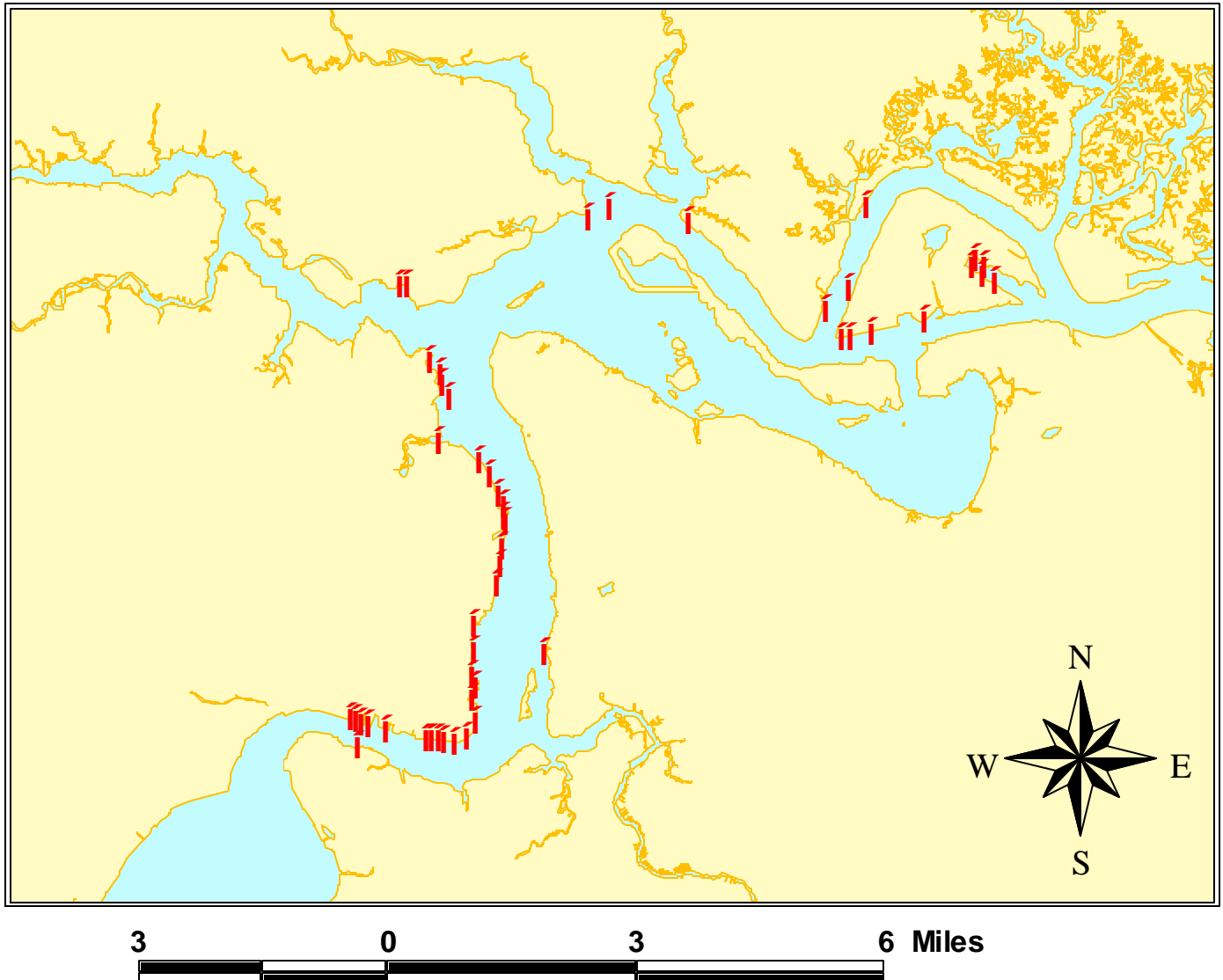
VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9100-9
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

# COTP Jacksonville AOR Northeast Florida



The boundary of the Jacksonville Marine Inspection Zone and Captain of the Port Zone starts at the Georgia coast at  $30^{\circ} 50'W$  ( $30^{\circ} 00'N$   $83^{\circ} 50'W$ ); mouth of the Fenholloway River, thence due north to a position  $30^{\circ} 15'N$   $83^{\circ} 50'W$ ; thence due west to a position  $30^{\circ} 15'N$   $84^{\circ} 45'W$ ; thence due north to the Florida-Georgia boundary at longitude  $84^{\circ} 45'W$ ; thence easterly along the Florida-Georgia boundary at longitude  $84^{\circ} 45'W$ ; thence easterly along the Florida-Georgia boundary to longitude  $83^{\circ} 00'W$ ; thence southeasterly to  $28^{\circ}00'N$   $81^{\circ} 30'W$ ; thence due south to  $26^{\circ} 00'N$   $81^{\circ} 30'W$ ; thence southwesterly to the southern tip of Cape Romano, FL. The western offshore boundary of the Tampa Captain of the Port Zone is a line bearing 199 T from the intersection of the Florida coast at  $30^{\circ} 00'N$ ,  $083^{\circ} 50'W$  Longitude to the offshore extent of the EEZ. The eastern offshore boundary is a line bearing 227 T from  $26^{\circ} 00'N$  Latitude  $081^{\circ} 30'W$  Longitude to the offshore extent of the EEZ.

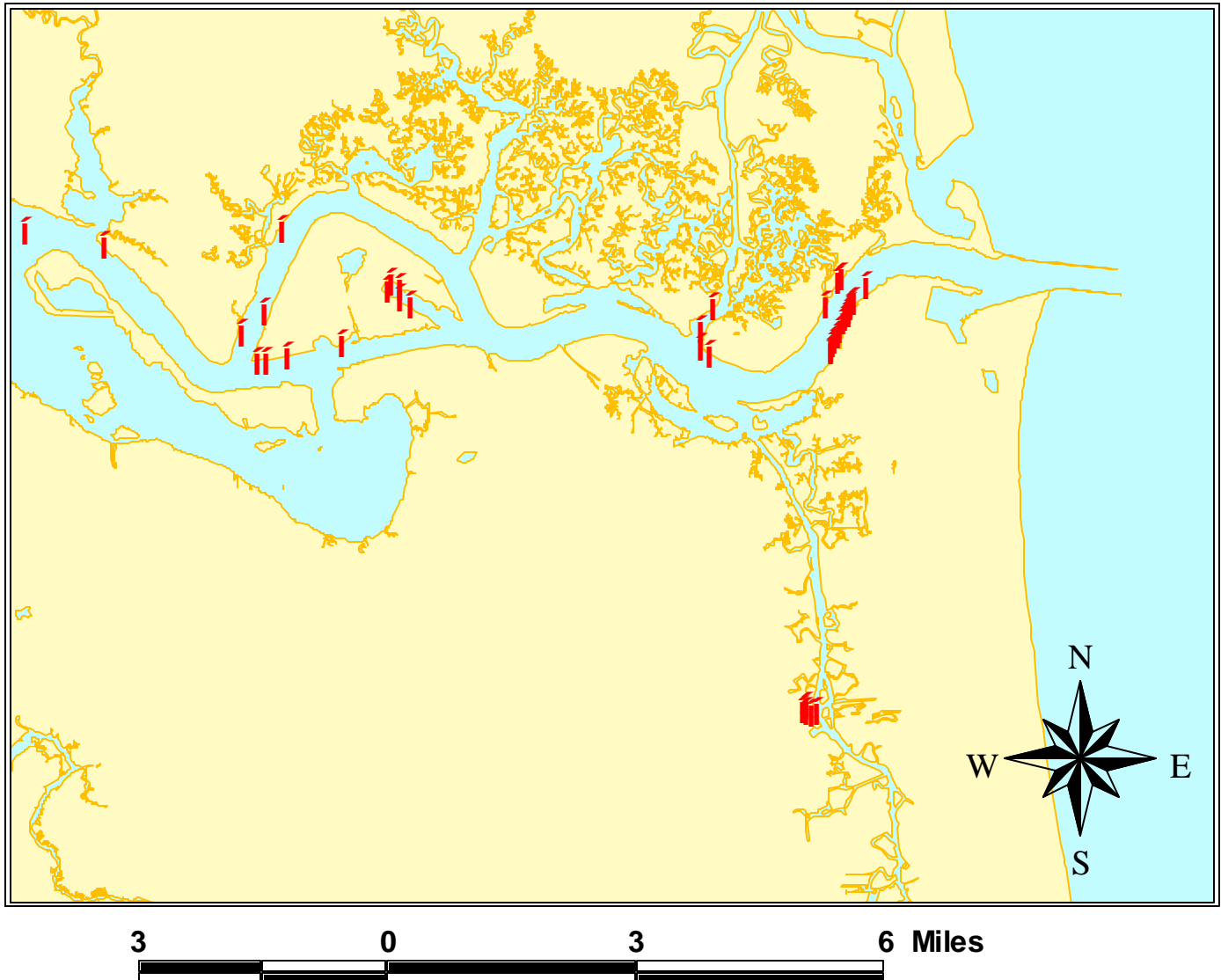
# Downtown Jacksonville



Most of the marine terminals are on the west side of the river about 21 miles above the entrance, just above the point where the river first turns southward. The deepwater port is the largest on the east coast of Florida.

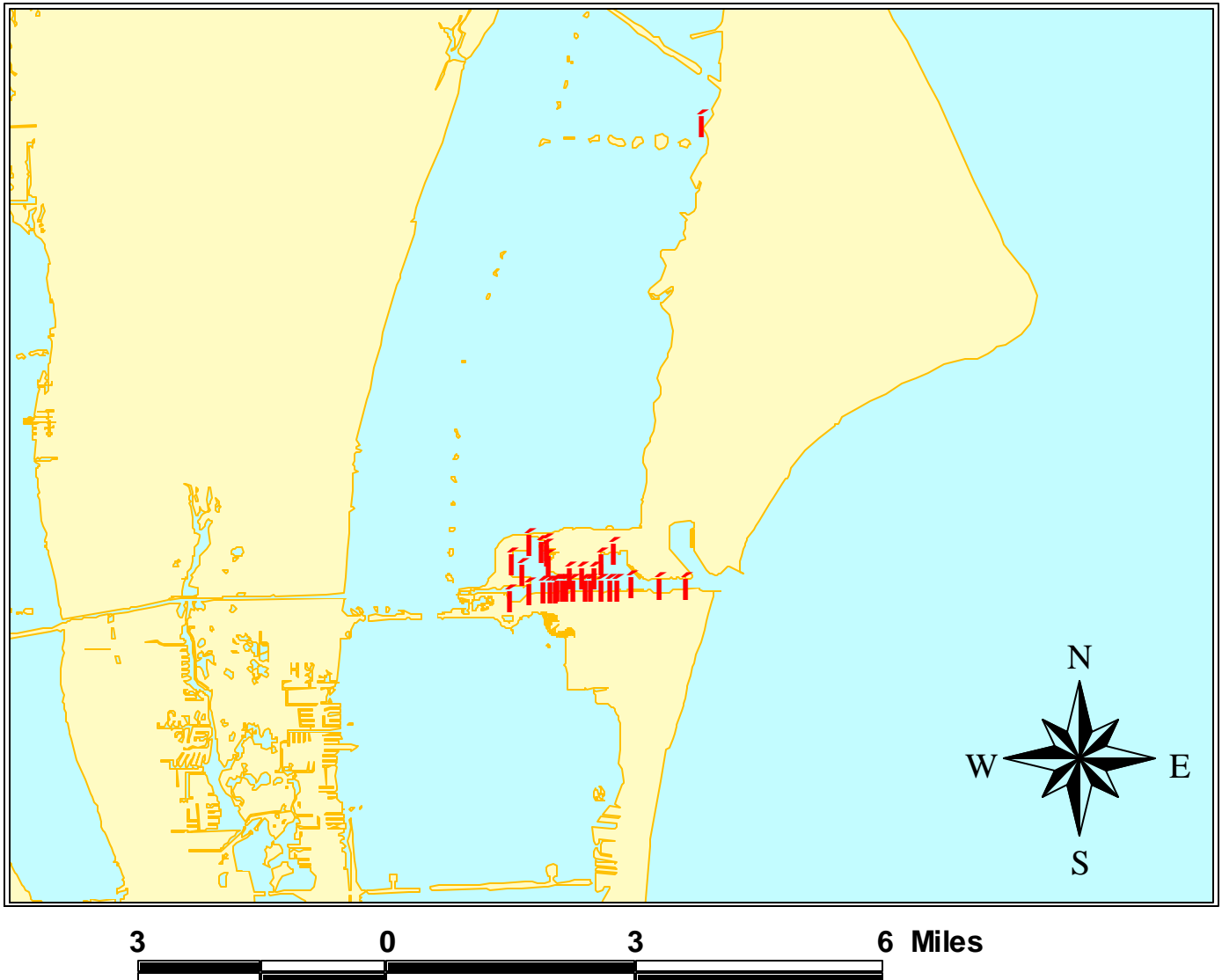


# Lower Saint Johns River



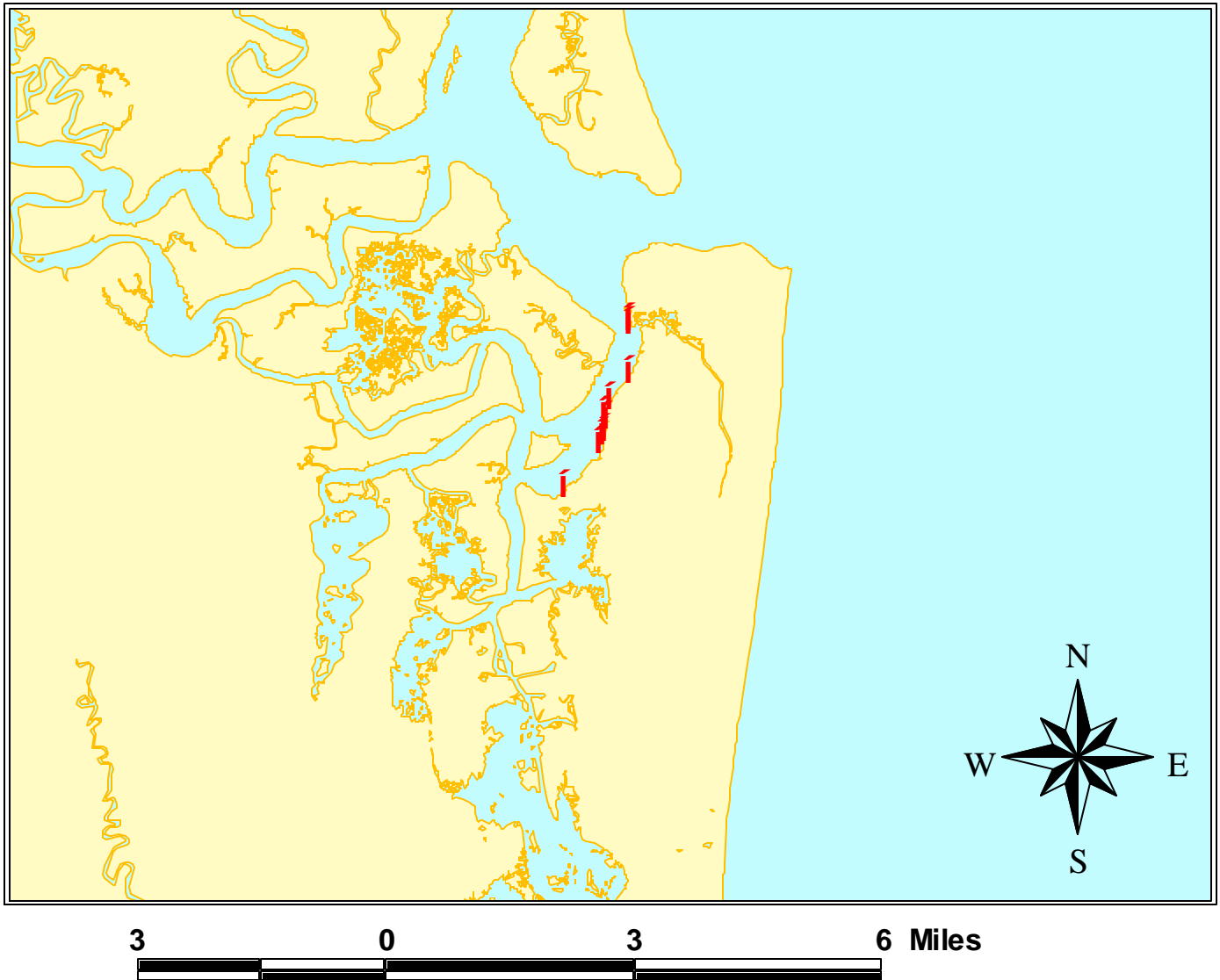
Blount Island, low and sandy with fringing marshes, is on the north side of the St. Johns River about 9 miles above the entrance. The Jacksonville Port Authority terminal near the southwestern tip of the island, and Gate Maritime Terminal in Back River (Gate Maritime Slipway) at the southeastern tip of the island have been described under Wharves for the Port of Jacksonville. Blount Island Channel, a cutoff bend of the St. Johns River, extends from the main river channel around the northern side of Blount Island and rejoins the main channel at the southwestern tip of the island. The channel is practically divided near its midpoint by four low fixed bridges with clearances of 18 feet horizontally and 5 feet vertically. Overhead power cables, with clearances of 175 feet, are on both sides of the southwestern-most highway bridge

# Port Canaveral



Port Canaveral is 4 miles southwest of Cape Canaveral Light and 150 miles south of the entrance to the St. Johns River. The city of Cape Canaveral is just southward of the port. The principal commodities handled in the harbor are petroleum products, cement, asphalt, salt, general cargo, citrus products, and newsprint. Commercial party fishing vessels, cruise ships, and many pleasure crafts operate from the port. Port Canaveral has commercial berths owned by the Port Authority. Middle and West Basins are used by commercial vessels as well as at the north and south sides of the Inner Reach; cruise ships usually berth in the West Basin.

# Port Fernandina



The Port of Fernandina is a general cargo terminal, specializing in forest products, and a container terminal facility. The terminal is served by the CSX Rail Road including double stack container trains and all major regional and national truck companies. The Port of Fernandina is located very near the Interstate Highway System, only 14 miles from I-95 connecting to the east/west I-10 corridor.

The Port of Fernandina is located on Amelia Island within the City of Fernandina Beach. Two paper mills, Smurfit-Stone and Rayonier are adjacent to the port. In addition, twelve other paper mills as far north as Tennessee and Virginia serve the Port of Fernandina. The major commodities include Kraft Liner Board, Wood Pulp and Lumber. In addition to breakbulk, the Port of Fernandina caters to the independent container liner services predominately serving the north/south trade lanes and the Caribbean. Major commodities include refrigerated and chilled cargos, auto parts, consumer goods and machinery.

## Tab E to Appendix 9500: Communications with Marinas

<b><i>JACKSONVILLE</i></b>	<b><i>PHONE</i></b>	<b><i>FAX</i></b>
<b>ARLINGTON MARINA</b> 5137 Arlington Rd. Jacksonville, FL 32211	(904)743-2628	(904)743-5366
<b>BEACH MARINE</b> 2315 Beach Blvd. Jacksonville Beach, FL 32250	(904)249-8200	(904)249-2050
<b>CLAPBOARD CREEK MARINA</b> <b>6220 Hecksher Drive</b> <b>Jacksonville, FL 32226</b>	<b>(904) 757-1135</b>	
<b>CAUSEWAY MARINE</b>	(904)247-5267	
<b>DOCTORS LAKE MARINA</b> 3108 U.S. Highway 17 South Orange Park, FL 32073	(904)264-0505	(904)264-6626
<b>EDWARD MARINA</b> 451-B Trout River Drive Jacksonville, FL 32208	(904)764-7022	
<b>EPPING FOREST YACHT CLUB</b> 1830 Epping Forest Dr. Jacksonville, FL 32217	(904)739-7150	(904)722-0054
<b>FLORIDA YACHT CLUB</b> 5210 Yacht Club Rd. Jacksonville, FL 32210	(904)387-1653	(904)389-9993
<b>MAYPORT MARINE</b> 4852 Ocean St.. Mayport, FL 32233	(904)246-8929	
<b>MULBERRY COVE MARINA</b>  NAS Jacksonville	(904)542-3260	(904)542-5941
<b>JULINGTON CREEK MARINA</b> 12807 San Jose Blvd. Jacksonville, FL 32223	(904)268-5117 (904) 268-5023	(904)260-9416
<b>LAMBS YACHT CENTER</b> 3376 Lakeshore Blvd. Jacksonville, FL 32210	(904)384-5577	(904)389-8346

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB E: 9500-1
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

<b>LIGHTHOUSE MARINE</b> 5434 San Juan Ave Jacksonville, FL 32210	(904)384-6995	(904)384-2306
<b>MANDARIN HOLIDAY MARINA</b> 12796 San Jose Blvd. Jacksonville, FL 32223	(904)268-1036	(904)880-2569
<b>RIVER CITY MARINE</b> (FORMERLY MANDARIN MARINA) 8940 San Jose Blvd. Jacksonville, FL 32217	(904)733-7502	(904)733-5726
<b>MONTYS MARINA</b> 4378 Ocean St. Mayport, FL 32233	(904)246-7575	No FAX
<b>ORTEGA RIVER BOAT YARD</b> 4451 Hershel St. Jacksonville, FL 32210	(904)387-5538	(904)387-6422
<b>ORTEGA RIVER YACHT CLUB</b> 4585 Lakeside Dr. Jacksonville, FL 32210	(904)389-1199	(904)389-5463
<b>PALM COVE MARINA</b> 14603 Beach Blvd. Jacksonville, FL 32225	(904)223-4757	(904)223-6601
<b>PELICAN CREEK MARINA</b>	(904)249-8979	
<b>RIVER CITY MARINA</b> 835 Museum Circle Jacksonville, FL 32207	(904)398-7918	(904)398-2099
<b>RUDDER CLUB OF JACKSONVILLE</b> 8533 Malaga Ave. Orange Park, FL 32073	(904)264-4094	Same
<b>SADLER POINT MARINA</b> 4669 Roosevelt Blvd. Jacksonville, FL 32210	(904)384-1383	(904)389-5187
<b>SEAFARERS MARINA</b> 455 Trout River Drive Jacksonville, FL 32208	(904)765-8152	
<b>TRAVIS BOATING CENTER</b> 8137 N. Main St. Jacksonville, FL 32208	(904)765-9925	(904)766-8300

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB E: 9500-2
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

**WEEKS MARINE** (904)387-1440 (904)387-5055  
 2652 Blanding Blvd.  
 Jacksonville, FL 32210

**WHITNEYS MARINE** (904)269-0027 (904)278-0243  
 3027 Highway 17  
 Orange Park, FL 32073

## **ST AUGUSTINE**

**COMANCHEE COVE YACHT BASIN** (904)829-5676 (904)829-0396  
 3070 Harbor Dr.  
 St. Augustine, FL 32084  
 1 800 345 9269

**CONCH HOUSE MARINA** (904)829-8646 (904)829-5414  
 57 Camares Ave.  
 St. Augustine, FL 32084  
 (904) 824-4347-1800 940 6256

**FISH ISLAND MARINA**  
**State Rd. 312**  
**St. Augustine, FL 32086** (904)471-1955

**HIDDEN HARBOR MARINA** (904) 829-0750 (904) 829-0750  
 10 Prawn St.  
 St. Augustine, FL 32084

**MARINELAND MARINA** (904)471-0087  
 176 Marina Dr.  
 St. Augustine, FL 32086

**MIKE BLACK MARINA** (904)829-8567  
 614 Euclid Ave.  
 St. Augustine, FL 32095

**OASIS BOATYARD** (904)824-2520  
**256 Riberia St.**  
**St. Augustine, FL 32084**

**OYSTER CREEK MARINA** (904) 827-0520  
**65 Lewis Blvd.**  
**St. Augustine, FL 32084**

**PACETTI MARINA** (904)264-1102 (904)284-9581  
 6550 State Road 13 North  
 St. Augustine, FL 32092

**SEBASTIAN HARBOR MARINA** (904)825-4666 (904)825-0229  
 975 S. Ponce de Leon Blvd.  
 St. Augustine, FL 32086

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB E: 9500-3
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

**ST. AUGUSTINE MARINE**  
404 S. Riberia St.  
St. Augustine, FL 32084

(904)824-4394

(904)824-9755

**ST. AUGUSTINE MUNICIPAL MARINE**  
100 Avenida Menendez  
St. Augustine, FL 32034

(904)825-1026

(904)825-1096

## **DAYTONA**

**ADVENTURE YACHT**  
3948 S. Peninsula Dr.  
Daytona Beach, FL 32127

(407)756-2180

(407)756-0693

**DAYTONA MARINA**  
645 S. Beach St.  
Daytona Beach, FL 32114

(407)252-6421

(407)253-8174

**ENGLISH JIMS**  
21 Ballough Rd.  
Daytona Beach, FL 32114

(407)253-5647  
or (407)253-5557

(407)252-7362

**FISHING COVE**  
111 N. Riverside Dr.  
New Smyrna, FL 32168

(407)428-7827

(407)428-2428

**HALIFAX HARBOR MARINA**  
450 Basin St.  
Daytona Beach, FL 32114

(407)253-0575

(407)258-4520

**LIGHTHOUSE BOATYARD**  
4958 S. Peninsula Dr.  
Ponce Inlet, FL 32127

(407)767-0683

(407)767-8814

**SEVEN SEAS**  
3300 S. Peninsula Dr.  
Daytona Beach, FL 32218

(407)761-3221

No FAX

## **FERNANDINA**

**AMELIA ISLAND YACHT BASIN**  
251 Creekside Dr.  
Amelia Island, FL 32034

(904)277-4615

(904)277-4025

**EGANS CREEK MARINA**

(904)261-3158

No FAX

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB E: 9500-4
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------



North 14<sup>th</sup> Street  
Fernandina Beach, FL 32034

**FERNANDINA BEACH MARINA**  
1 Front St.  
Fernandina Beach, FL 32034

(904)261-0355

(904)277-8491

**TIGER POINT MARINA & BOAT WORKS**  
112 N.6<sup>th</sup> St.  
Fernandina Beach, FL 32034

(904)261-3158

Same

**TRADEWINDS**  
1 Front St.  
Fernandina Beach, FL 32034

(904)261-9486

No FAX

### **OTHERS**

**BOATHOUSE MARINA**  
329 River St.  
Palatka, FL 32177

(386)328-2944

**GIBSON DRYDOCKS**  
P.O. Box 293  
San Mateo, FL 32187

(407)325-5502

No FAX

**GREEN COVE MARINA**  
851 Bulkhead Rd.  
Green Cove Springs, FL 32034

(904)284-1811

(904)284-1866

**MIDWAY MARINA**  
25127 Pearl St.  
Astor, FL 32102

(407)478-2333

Same

**OSPREY COVE CC BOAT DOCKS**  
123 Osprey Dr.  
St. Marys, GA 31558

(912)882-5555

(912)882-4004

**PALM COAST MARINA**  
200 Club House Dr.  
Palm Coast, FL 32137

(386)446-6370

(386)445-9563

**SANFORD BOAT WORKS & MARINA**  
4130 Celery Ave.  
Sanford, FL 32771

(407)322-6613

(407)322-6616

**SHELL HARBOR MARINA**  
140 Shell Harbour Rd.  
Satsuma, FL 32189

(407)467-2330

(407)467-7100

**LAST UPDATED 18FEB03**

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB E: 9500-5
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab F to Appendix 9500: Communications with County Emergency Management (EOCs)

### Nassau County Emergency Management

Thomas Kochheiser, Director  
Nassau County Emergency Management  
11 North 14th Street, Box 12  
Fernandina Beach, Florida 32034  
Phone: 904-491-7550  
Fax: 904-491-3628  
Suncom: 848-5732  
e-mail: [ncem@nassaucountyfl.com](mailto:ncem@nassaucountyfl.com)  
[Nassau County Emergency Management Website](#)

### Duval County Emergency Management

Robert Patterson, Director  
Duval County Emergency Management  
515 North Julia St.  
Jacksonville, Florida 32202  
Phone: 904-630-2472  
Fax: 904-630-0600  
Suncom: N/A  
e-mail: [cpatters@coj.net](mailto:cpatters@coj.net)  
[Duval County Emergency Management Website](#)

### Baker County Emergency Management

Rick Clark, Director  
Baker County Emergency Management  
1190 West Macclenny Avenue  
Macclenny, Florida 32063  
Phone: 904-259-6111  
Fax: 904-259-3923  
Suncom: N/A  
e-mail: [bcem@setel.net](mailto:bcem@setel.net)  
[Baker County Emergency Management Website](#)

VERSION DATE	<a href="#">VER 1.1</a> <a href="#">26 MAY 04</a>	CLASSIFICATION: <a href="#">UNCLAS</a>	CONTROLLING AUTHORITY	<a href="#">USCG</a> <a href="#">MSO JAX</a>	ISSUING AUTHORITY	<a href="#">CAPT</a> <a href="#">D.L. LERSCH</a>	PAGE	TAB F: 9500-1
-----------------	--	---	--------------------------	---	----------------------	---	------	------------------

**Union County  
Emergency Management**

Tommy Thomas, Director  
Union County Emergency Management  
58 Northwest 1st Street  
Lake Butler, Florida 32054  
Phone: 386-496-4330  
Fax: 386-496-3226  
Suncom: n/a  
e-mail: [ucoem@alltel.net](mailto:ucoem@alltel.net)  
[Union County Emergency Management Website](#)

**Bradford County  
Emergency Management**

William E. "Bill" Dampier, Director  
Bradford County Emergency Management  
945-B N. Temple Ave.  
Starke, Florida 32091  
Phone: 904-966-6336  
Fax: 904-966-6169  
Suncom: N/A  
e-mail: [bill\\_dampier@bradford-co-fla.org](mailto:bill_dampier@bradford-co-fla.org)  
[Bradford County Emergency Management Website](#)

**Clay County  
Emergency Management**

James Corbin Jr., Director  
Clay County Emergency Management  
1 Doctors Drive  
Green Cove Springs, Florida 32043-3128  
Phone: 904-284-7703  
Fax: 904-529-2273  
Suncom: N/A  
e-mail: [jim.corbin@co.clay.fl.us](mailto:jim.corbin@co.clay.fl.us)  
[Clay County Emergency Management Website](#)

VERSION DATE	<a href="#">VER 1.1</a> <a href="#">26 MAY 04</a>	CLASSIFICATION: <a href="#">UNCLAS</a>	CONTROLLING AUTHORITY	<a href="#">USCG</a> <a href="#">MSO JAX</a>	ISSUING AUTHORITY	<a href="#">CAPT</a> <a href="#">D.L. LERSCH</a>	PAGE	TAB F: 9500-2
-----------------	--	---	--------------------------	---	----------------------	---	------	------------------

**St. Johns County  
Emergency Management**

E.R. Ashton, Director  
St. Johns County Emergency Management  
4455 Avenue "A", Suite 102  
St. Augustine, Florida 32095  
Phone: 904-824-5550  
Fax: 904-824-9920  
Suncom: 865-2644  
e-mail: [emgmgt@co.st-johns.fl.us](mailto:emgmgt@co.st-johns.fl.us)  
[St. Johns County Emergency Management Website](#)

**Putnam County  
Emergency Management**

Douglas C. Stewart, Director  
Putnam County Emergency Management  
120 Orie Griffin Blvd  
Palatka, Florida 32177-1416  
Phone: 386-329-0379  
Fax: 386-329-0897  
Suncom: 860-0379  
e-mail: [dem@putnam-fl.com](mailto:dem@putnam-fl.com)  
[Putnam County Emergency Management Website](#)

**Marion County  
Emergency Management**

Lt. Chip Wildy, Director  
Marion County Emergency Management  
Post Office Box 1987  
Ocala, Florida 34478-1987  
Phone: 352-622-3205  
Fax: 352-369-6762  
Suncom: n/a  
e-mail: [cwildy@sheriff.marioncountyfl.org](mailto:cwildy@sheriff.marioncountyfl.org)  
[Marion County Emergency Management Website](#)

VERSION DATE	<a href="#">VER 1.1</a> <a href="#">26 MAY 04</a>	CLASSIFICATION: <a href="#">UNCLAS</a>	CONTROLLING AUTHORITY	<a href="#">USCG</a> <a href="#">MSO JAX</a>	ISSUING AUTHORITY	<a href="#">CAPT</a> <a href="#">D.L. LERSCH</a>	PAGE	TAB F: 9500-3
-----------------	--	---	--------------------------	---	----------------------	---	------	------------------

**Flagler County  
Emergency Management**

Douglas Wright, Director  
Flagler County Emergency Management  
1200 East Boulevard #8  
Bunnell, Florida 32110-5918  
Phone: 386-437-7381  
Fax: 386-437-7489  
Suncom: 370-7381  
e-mail: [dwright@flagleremergency.com](mailto:dwright@flagleremergency.com)  
[Flagler County Emergency Management Website](#)

**Volusia County  
Emergency Management**

James R. Ryan, Director  
Volusia County Emergency Management  
49 Keyton Avenue  
Daytona Beach, Florida 32124  
Phone: 386-254-1500  
Fax: 386-248-1742  
Suncom: 377-1500  
e-mail: [jryan@co.volusia.fl.us](mailto:jryan@co.volusia.fl.us)  
[Volusia County Emergency Management Website](#)

**Lake County  
Emergency Management**

Butch Whitehead, Director  
Lake County Emergency Management  
315 West Main Street, Suite 411  
Tavares, Florida 34778  
Phone: 352-343-9420  
Fax: 352-343-9728  
Suncom: n/a  
e-mail: [BWhitehead@co.lake.fl.us](mailto:BWhitehead@co.lake.fl.us)  
[Lake County Emergency Management Website](#)

VERSION DATE	<a href="#">VER 1.1</a> <a href="#">26 MAY 04</a>	CLASSIFICATION: <a href="#">UNCLAS</a>	CONTROLLING AUTHORITY	<a href="#">USCG</a> <a href="#">MSO JAX</a>	ISSUING AUTHORITY	<a href="#">CAPT</a> <a href="#">D.L. LERSCH</a>	PAGE	TAB F: 9500-4
-----------------	--	---	--------------------------	---	----------------------	---	------	------------------

**Seminole County  
Emergency Management**

Ken Roberts, Director  
Seminole County Emergency Management  
150 Bush Boulevard  
Sanford, Florida 32773  
Phone: 407-665-5102 E  
Fax: 407-665-5135  
Suncom: n/a  
e-mail: [kroberts@co.seminole.fl.us](mailto:kroberts@co.seminole.fl.us)  
[Seminole County Emergency Management Website](#)

**Orange County  
Emergency Management**

Renzy Hanshaw, Executive Director  
Orange County Emergency Management  
Post Office Box 5879  
Winter Park, Florida 32793-5879  
Phone: 407-836-9151  
Fax: 407-836-9147  
Suncom: n/a  
e-mail: [ocoem@ocfl.net](mailto:ocoem@ocfl.net)  
[Orange County Emergency Management Website](#)

**Brevard County  
Emergency Management**

Robert Lay, Director  
Brevard County Emergency Management  
1746 Cedar Street  
Rockledge, Florida 32955  
Phone: 321-637-6670  
Fax: 321-633-1738  
Suncom: 359-1770  
e-mail: [bob.lay@brevardcounty.us](mailto:bob.lay@brevardcounty.us)  
[Brevard County Emergency Management Website](#)

**Osceola County  
Emergency Management**

Cheryl Grabowski, Director  
Osceola County Emergency Management  
320 N. Beaumont Avenue  
Kissimmee, Florida 34741  
Phone: 407-343-7000  
Fax: 407-343-6873  
e-mail: [cgra2@osceola.org](mailto:cgra2@osceola.org)

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB F: 9500-5
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab G to Appendix 9500: Communications with Waterway Users (Boaters)

<u>(Required)</u> Subscriber Name	<u>(Optional)</u> Street	<u>(Required)</u> City	<u>ST</u>	<u>Zip</u>	<u>(Optional)</u> Phone	<u>(Required)</u> E-mail POC	<u>(Required)</u> Fax POC	<u>Subscription</u> Date	<u>Date</u> <u>Last</u> <u>Verified</u>



## Tab H to Appendix 9500: (UNCLAS) MSIB MARSEC TWO



**COAST GUARD**  
**MARINE SAFETY OFFICE**  
**JACKSONVILLE**



7820 Arlington Expressway Suite 400  
Jacksonville, FL 32211-7445  
Phone: (904) 232-2640  
Fax: (904) 232-1014  
[www.uscg.mil/d7/units/mso-jax](http://www.uscg.mil/d7/units/mso-jax)

### MARINE SAFETY INFORMATION BULLETIN XX-04

Month DD, 2004

#### **Homeland Security Advisory System (HSAS)** **Threat Level: HIGH (Orange)** **Maritime Security Level: TWO**

The Department of Homeland Security in consultation with the Homeland Security Council has made the decision to raise the national threat level from an Elevated to High risk of terrorist attack to **Level Orange**. The U.S. Intelligence Community has received a substantial increase in the volume of threat related intelligence reports. These credible sources suggest the possibility of attacks against the homeland around the *(holiday/event/etc.)* and beyond. Accordingly, the Commandant of the Coast Guard and I, as the Federal Maritime Security Coordinator, have raised the port security level to **MARSEC TWO** for all ports, waterways, and coastline in Northeast and Eastern Central Florida including ports along the St. Marys River in Georgia.

I recommend Port Authorities, facility operators, vessel operators, and infrastructure owners and operators review their security plans/procedures and implement MARSEC TWO measures. I also ask all operators **conduct an OPERATIONAL PAUSE** while all spaces and operations ashore and afloat are reviewed. The Operational Pause should include a review of all personnel at your facility or aboard your vessel, and a routine search for suspicious or unusual packages or planted devices. I do not believe the Operational Pause will require you to halt or disrupt your routine operations, but I leave that decision to your discretion in view of the possible safety issues involved with searching while operations are ongoing. Please report the all-clear as soon as possible and no later than two hours after you receive this MSIB to the USCG Integrated Command Center via our web-report form. Point your browser to:

[http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication\\_email.htm](http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication_email.htm)

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB H: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab H to Appendix 9500: (UNCLAS) MSIB MARSEC TWO

If (and only if) you are unable to access the Internet, please report the all-clear to the Coast Guard ICC at 904-247-7318. I ask that you repeat the review/search procedures every 12 hours while MARSEC TWO is maintained, and please report **any** anomalies to local law enforcement, the Coast Guard ICC (**904-247-7318**) **and** the National Response Center (**1-800-424-8802**).

Report **suspicious activity** or **security breaches** immediately to 911, the Coast Guard ICC at (904) 247-7318 and the National Response Center at (800) 422-8802.

We also draw your attention to the Department of Homeland Security's web site for additional information about the specific threats and protective measures which all members of the maritime public should implement:

<http://www.dhs.gov/dhspublic/display?theme=29>

[ (optional) *For those port stakeholders with questions or concerns about this MARSEC TWO heightened security evolution, the Federal Maritime Security Coordinator has scheduled emergency Port Security Committee meetings in the Port of Jacksonville and the Port of Canaveral for Month XX, 2004. Attendance at these meetings is not mandatory, but may be of value in further explaining the threats, requested security actions, and likely effects on commerce and recreational boating. General public meetings have been scheduled for:*

JMTX Port Security Committee	X:XX p.m.	JAXPORT Office Building
Port Canaveral Security Committee	X:XX p.m.	Port Authority Board Room

*Please frequently check our website, **www.uscg.mil/d7/units/mso-jax** for updates. ]*

All port stakeholders are requested to increase the awareness of all employees and personnel involved and report any suspicious activities to local law enforcement, the Coast Guard ICC (904-247-7318) **and** the National Response Center (**1-800-424-8802**). Future changes in MARSEC LEVEL will also be announced by bulletins like this and through the Port Security Committees.

//s//

D. L. LERSCH  
Captain, U.S. Coast Guard  
Officer in Charge, Marine Inspection  
Jacksonville, Florida

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB H: 9500-2
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab I to Appendix 9500: MSIB MARSEC TWO to ONE



**COAST GUARD**  
**MARINE SAFETY OFFICE**  
**JACKSONVILLE**



7820 Arlington Expressway Suite 400  
Jacksonville, FL 32211-7445  
Phone: (904) 232-2640  
Fax: (904) 232-1014  
[www.uscg.mil/d7/units/mso-jax](http://www.uscg.mil/d7/units/mso-jax)

### **MARINE SAFETY INFORMATION BULLETIN 01-04**

January 9, 2004

#### **Homeland Security Advisory System (HSAS) Threat Level: ELEVATED (Yellow) Maritime Security Condition: ONE**

Following a review of intelligence and an assessment of threats by the intelligence community, the Department of Homeland Security, in consultation with the Homeland Security Council, has made the decision to lower the threat advisory level to an elevated risk of terrorist attack, or "**yellow level**." Accordingly, the Maritime Security Condition (**MARSEC**) level in the Port of Jacksonville, Fernandina, and Canaveral has been returned to **MARSEC ONE**.

The lowering of the threat and MARSEC level is not a signal to government, law enforcement, the port, or citizens that the danger of a terrorist attack is passed. We must be vigilant and alert to the possibility that al-Qaida and those sympathetic to their cause, as well as former Iraqi-regime state agents and affiliated organizations, may attempt to conduct attacks against the U. S. or our interests abroad. For this reason, and for the safety and security of our nation, Americans must continue to be alert, undaunted and prepared to respond to a significant risk of terrorist attacks.

I extend my appreciation to all stakeholders for their patience, resolve, and the level of effort put forth during this period of heightened security. The signal we have sent our enemies over the past few weeks has been clear. We will continue to resolutely defend our Nation and its freedom. Through your collective efforts we send a signal to those who would do us harm that America stands alert, united, and prepared.

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB I: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab I to Appendix 9500: MSIB MARSEC TWO to ONE

D. L. LERSCH  
Captain, U.S. Coast Guard  
Captain of the Port

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB I: 9500-2
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab J to Appendix 9500: MSIB MARSEC THREE



**COAST GUARD**  
**MARINE SAFETY OFFICE**  
**JACKSONVILLE**



7820 Arlington Expressway Suite 400  
Jacksonville, FL 32211-7445  
Phone: (904) 232-2640  
Fax: (904) 232-1014  
[www.uscg.mil/d7/units/mso-jax](http://www.uscg.mil/d7/units/mso-jax)

### MARINE SAFETY INFORMATION BULLETIN XX-04

Month DD, 2004

#### **Homeland Security Advisory System (HSAS)** **Threat Level: EXTREME (RED)** **Maritime Security Level: THREE**

The Department of Homeland Security in consultation with the Homeland Security Council has made the decision to raise the national threat level from an Elevated to an Extreme risk of terrorist attack (**Level Red**). The U.S. Intelligence Community has received credible intelligence reports. These credible reports suggest the possibility of attacks against (target if known or the homeland) around the (time period). Accordingly, the Commandant of the Coast Guard and I, as the Federal Maritime Security Coordinator, have raised the port security level to **MARSEC THREE** for all ports, waterways, and coastline in Northeast and Eastern Central Florida including ports along the St. Marys River in Georgia.

The ports of Jacksonville, Fernandina, and Canaveral are closed to all traffic. No vessels are authorized to transit inbound or outbound during **MARSEC THREE**.

I recommend Port Authorities, facility operators, vessel operators, and infrastructure owners and operators review their security plans/procedures and implement **MARSEC THREE** measures. I also ask all operators **conduct an OPERATIONAL PAUSE** while all spaces and operations ashore and afloat are reviewed. The Operational Pause should include a review of all personnel at your facility or aboard your vessel, and a routine search for suspicious or unusual packages or planted devices. I do not believe the Operational Pause will require you to halt or disrupt your routine operations, but I leave that decision to your discretion in view of the possible safety issues involved with searching while operations are ongoing. Please report the all-clear as soon as possible and no later than two hours after you receive this MSIB to the USCG Integrated Command Center via our web-report form. Point your browser to:

[http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication\\_email.htm](http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication_email.htm)

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB J: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab J to Appendix 9500: MSIB MARSEC THREE

If (and only if) you are unable to access the Internet, please report the all-clear to the Coast Guard ICC at 904-247-7318. I ask that you repeat the review/search procedures every 12 hours while MARSEC TWO is maintained, and please report **any** anomalies to local law enforcement, the Coast Guard ICC (**904-247-7318**) **and** the National Response Center (**1-800-424-8802**).

Report **suspicious activity** or **security breaches** immediately to 911, the Coast Guard ICC at (904) 247-7318 and the National Response Center at (800) 422-8802.

We also draw your attention to the Department of Homeland Security's web site for additional information about the specific threats and protective measures which all members of the maritime public should implement:

<http://www.dhs.gov/dhspublic/display?theme=29>

[ (optional) *For those port stakeholders with questions or concerns about this MARSEC TWO heightened security evolution, the Federal Maritime Security Coordinator has scheduled emergency Port Security Committee meetings in the Port of Jacksonville and the Port of Canaveral for Month XX, 2004. Attendance at these meetings is not mandatory, but may be of value in further explaining the threats, requested security actions, and likely effects on commerce and recreational boating. General public meetings have been scheduled for:*

JMTX Port Security Committee	X:XX p.m.	JAXPORT Office Building
Port Canaveral Security Committee	X:XX p.m.	Port Authority Board Room

*Please frequently check our website, **www.uscg.mil/d7/units/mso-jax** for updates. ]*

All port stakeholders are requested to increase the awareness of all employees and personnel involved and report any suspicious activities to local law enforcement, the Coast Guard ICC (904-247-7318) **and** the National Response Center (**1-800-424-8802**). Future changes in MARSEC LEVEL will also be announced by bulletins like this and through the Port Security Committees.

//s//

D. L. LERSCH  
Captain, U.S. Coast Guard  
Officer in Charge, Marine Inspection  
Jacksonville, Florida

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB J: 9500-2
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab K to Appendix 9500: MSIB MARSEC TWO to THREE



**COAST GUARD**  
**MARINE SAFETY OFFICE**  
**JACKSONVILLE**



7820 Arlington Expressway Suite 400  
Jacksonville, FL 32211-7445  
Phone: (904) 232-2640  
Fax: (904) 232-1014  
[www.uscg.mil/d7/units/mso-jax](http://www.uscg.mil/d7/units/mso-jax)

### MARINE SAFETY INFORMATION BULLETIN XX-04

Month DD, 2004

#### **Homeland Security Advisory System (HSAS)** **Threat Level: EXTREME (RED)** **Maritime Security Level: THREE**

The Department of Homeland Security in consultation with the Homeland Security Council has made the decision to raise the national threat level from a High to an Extreme risk of terrorist attack (**Level Red**). The U.S. Intelligence Community has received credible intelligence reports. These credible reports suggest the possibility of attacks against (target if known or the homeland) around the (time period). Accordingly, the Commandant of the Coast Guard and I, as the Federal Maritime Security Coordinator, have raised the port security level to **MARSEC THREE** for all ports, waterways, and coastline in Northeast and Eastern Central Florida including ports along the St. Marys River in Georgia.

The ports of Jacksonville, Fernandina, and Canaveral are closed to all traffic. No vessels are authorized to transit inbound or outbound during **MARSEC THREE**.

I recommend Port Authorities, facility operators, vessel operators, and infrastructure owners and operators review their security plans/procedures and implement **MARSEC THREE** measures. I also ask all operators **conduct an OPERATIONAL PAUSE** while all spaces and operations ashore and afloat are reviewed. The Operational Pause should include a review of all personnel at your facility or aboard your vessel, and a routine search for suspicious or unusual packages or planted devices. I do not believe the Operational Pause will require you to halt or disrupt your routine operations, but I leave that decision to your discretion in view of the possible safety issues involved with searching while operations are ongoing. Please report the all-clear as soon as possible and no later than two hours after you receive this MSIB to the USCG Integrated Command Center via our web-report form. Point your browser to:

[http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication\\_email.htm](http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication_email.htm)

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB K: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------



## Tab K to Appendix 9500: MSIB MARSEC TWO to THREE

If (and only if) you are unable to access the Internet, please report the all-clear to the Coast Guard ICC at 904-247-7318. I ask that you repeat the review/search procedures every 12 hours while MARSEC TWO is maintained, and please report **any** anomalies to local law enforcement, the Coast Guard ICC (**904-247-7318**) **and** the National Response Center (**1-800-424-8802**).

Report **suspicious activity** or **security breaches** immediately to 911, the Coast Guard ICC at (904) 247-7318 and the National Response Center at (800) 422-8802.

We also draw your attention to the Department of Homeland Security's web site for additional information about the specific threats and protective measures which all members of the maritime public should implement:

<http://www.dhs.gov/dhspublic/display?theme=29>

[ (optional) *For those port stakeholders with questions or concerns about this MARSEC TWO heightened security evolution, the Federal Maritime Security Coordinator has scheduled emergency Port Security Committee meetings in the Port of Jacksonville and the Port of Canaveral for Month XX, 2004. Attendance at these meetings is not mandatory, but may be of value in further explaining the threats, requested security actions, and likely effects on commerce and recreational boating. General public meetings have been scheduled for:*

JMTX Port Security Committee	X:XX p.m.	JAXPORT Office Building
Port Canaveral Security Committee	X:XX p.m.	Port Authority Board Room

*Please frequently check our website, **www.uscg.mil/d7/units/mso-jax** for updates. ]*

All port stakeholders are requested to increase the awareness of all employees and personnel involved and report any suspicious activities to local law enforcement, the Coast Guard ICC (904-247-7318) **and** the National Response Center (**1-800-424-8802**). Future changes in MARSEC LEVEL will also be announced by bulletins like this and through the Port Security Committees.

//s//

D. L. LERSCH  
Captain, U.S. Coast Guard  
Officer in Charge, Marine Inspection  
Jacksonville, Florida

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB K: 9500-2
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab L to Appendix 9500: MSIB MARSEC THREE to TWO



**COAST GUARD**  
**MARINE SAFETY OFFICE**  
**JACKSONVILLE**



7820 Arlington Expressway Suite 400  
Jacksonville, FL 32211-7445  
Phone: (904) 232-2640  
Fax: (904) 232-1014  
[www.uscg.mil/d7/units/mso-jax](http://www.uscg.mil/d7/units/mso-jax)

### MARINE SAFETY INFORMATION BULLETIN XX-04

Month DD, 2004

#### **Homeland Security Advisory System (HSAS)** **Threat Level: EXTREME (RED)** **Maritime Security Level: THREE**

The Department of Homeland Security in consultation with the Homeland Security Council has made the decision to lower the national threat level from an Extreme to a High risk of terrorist attack (**Level Orange**). The U.S. Intelligence Community has received a substantial increase in the volume of threat related intelligence reports. These credible reports suggest the possibility of attacks against the homeland around the *(time period)*. Accordingly, the Commandant of the Coast Guard and I, as the Federal Maritime Security Coordinator, have lowered the port security level to **MARSEC TWO** for all ports, waterways, and coastline in Northeast and Eastern Central Florida including ports along the St. Marys River in Georgia.

I recommend Port Authorities, facility operators, vessel operators, and infrastructure owners and operators review their security plans/procedures and implement **MARSEC TWO** measures. I also ask all operators **conduct an OPERATIONAL PAUSE** while all spaces and operations ashore and afloat are reviewed. The Operational Pause should include a review of all personnel at your facility or aboard your vessel, and a routine search for suspicious or unusual packages or planted devices. I do not believe the Operational Pause will require you to halt or disrupt your routine operations, but I leave that decision to your discretion in view of the possible safety issues involved with searching while operations are ongoing. Please report the all-clear as soon as possible and no later than two hours after you receive this MSIB to the USCG Integrated Command Center via our web-report form. Point your browser to:

[http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication\\_email.htm](http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication_email.htm)

If (and only if) you are unable to access the Internet, please report the all-clear to the Coast Guard ICC at 904-247-7318. I ask that you repeat the review/search procedures every 12

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB L: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab L to Appendix 9500: MSIB MARSEC THREE to TWO

hours while MARSEC TWO is maintained, and please report **any** anomalies to local law enforcement, the Coast Guard ICC (904-247-7318) **and** the National Response Center (1-800-424-8802).

Report **suspicious activity** or **security breaches** immediately to 911, the Coast Guard ICC at (904) 247-7318 and the National Response Center at (800) 422-8802.

We also draw your attention to the Department of Homeland Security's web site for additional information about the specific threats and protective measures which all members of the maritime public should implement:

<http://www.dhs.gov/dhspublic/display?theme=29>

[ (optional) *For those port stakeholders with questions or concerns about this MARSEC TWO heightened security evolution, the Federal Maritime Security Coordinator has scheduled emergency Port Security Committee meetings in the Port of Jacksonville and the Port of Canaveral for Month XX, 2004. Attendance at these meetings is not mandatory, but may be of value in further explaining the threats, requested security actions, and likely effects on commerce and recreational boating. General public meetings have been scheduled for:*

JMTX Port Security Committee	X:XX p.m.	JAXPORT Office Building
Port Canaveral Security Committee	X:XX p.m.	Port Authority Board Room

*Please frequently check our website, **www.uscg.mil/d7/units/mso-jax** for updates. ]*

All port stakeholders are requested to increase the awareness of all employees and personnel involved and report any suspicious activities to local law enforcement, the Coast Guard ICC (904-247-7318) **and** the National Response Center (1-800-424-8802). Future changes in MARSEC LEVEL will also be announced by bulletins like this and through the Port Security Committees.

//s//

D. L. LERSCH  
Captain, U.S. Coast Guard  
Officer in Charge, Marine Inspection  
Jacksonville, Florida

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB L: 9500-2
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab M to Appendix 9500: BNTM MARSEC ONE

FM COGARD MSO JACKSONVILLE FL  
TO COMCOGARDGRU MAYPORT FL  
INFO COMDT COGARD WASHINGTON DC  
BT

UNCLAS //N16502//

SUBJ: MARINE INFORMATION BROADCAST

1. REQUEST GROUP MAYPORT BROADCAST UNSCHEDULED BROADCAST VIA VHF-FM  
COMMENCING UPON RECEIPT UNTIL CANCELLED.

A. FLORIDA - JACKSONVILLE - FERNANDINA- CANAVERAL

"THIS IS A U.S. COAST GUARD HOMELAND SECURITY ALERT. THE MARITIME  
SECURITY LEVEL IN THE PORTS OF JACKSONVILLE, FERNANDINA, AND CANAVERAL  
HAS BEEN LOWERED TO LEVEL ONE. FACILITIES AND COMMERCIAL VESSELS ARE  
STILL ADVISED TO MAINTAIN A HEIGHTENED SECURITY AWARENESS."

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB M: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab N to Appendix 9500: BNTM MARSEC TWO

FM COGARD MSO JACKSONVILLE FL  
TO COMCOGARDGRU MAYPORT FL  
INFO COMDT COGARD WASHINGTON DC  
BT

UNCLAS //N16502//

SUBJ: MARINE INFORMATION BROADCAST

1. REQUEST GROUP MAYPORT BROADCAST UNSCHEDULED BROADCAST VIA VHF-FM  
COMMENCING UPON RECEIPT UNTIL CANCELLED.

A. FLORIDA - JACKSONVILLE - FERNANDINA- CANAVERAL

"THIS IS A U.S. COAST GUARD HOMELAND SECURITY ALERT. THE MARITIME  
SECURITY LEVEL IN THE PORTS OF JACKSONVILLE, FERNANDINA, AND CANAVERAL  
HAS BEEN RAISED TO LEVEL TWO. COMMERCIAL VESSELS ARE ADVISED TO  
IMPLEMENT HEIGHTENED SECURITY PROCEDURES WHILE IN THESE PORTS. THIS  
HEIGHTENED SECURITY LEVEL WILL REMAIN IN EFFECT UNTIL FURTHER NOTICE."

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB N: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab O to Appendix 9500: BNTM MARSEC THREE

FM COGARD MSO JACKSONVILLE FL  
TO COMCOGARDGRU MAYPORT FL  
INFO COMDT COGARD WASHINGTON DC  
BT

UNCLAS //N16502//

SUBJ: MARINE INFORMATION BROADCAST

1. REQUEST GROUP MAYPORT BROADCAST UNSCHEDULED BROADCAST VIA VHF-FM  
COMMENCING UPON RECEIPT UNTIL CANCELLED.

A. FLORIDA - JACKSONVILLE - FERNANDINA- CANAVERAL

"THIS IS A U.S. COAST GUARD HOMELAND SECURITY ALERT. THE MARITIME  
SECURITY LEVEL IN THE PORTS OF JACKSONVILLE, FERNANDINA, AND CANAVERAL  
HAS BEEN RAISED TO LEVEL THREE. THE PORTS OF JACKSONVILLE, FERNANDINA,  
AND CANAVERAL ARE CLOSED. THIS HEIGHTENED SECURITY LEVEL WILL REMAIN IN  
EFFECT UNTIL FURTHER NOTICE."

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO Jax	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB O: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

## Tab Q to Appendix 9500: MARSEC COMMUNICATION E-MAIL TEMPLATE

MARSEC COMMUNICATION E-mail Title FORMAT:

[MARSEC LEVEL] / [ACTION STATUS] / [PORT/CITY] / [ENTITY TYPE] / [ENTITY NAME] / [DATE] / [TIME]

MARSEC LEVEL Choices (Picklist):

MARSEC ONE  
MARSEC TWO  
MARSEC THREE

ACTION STATUS Choices (Picklist):

LEVEL CHANGE ACKNOWLEDGED  
OPERATIONAL PAUSE COMPLETE - ALL CLEAR  
LEVEL FULLY ATTAINED  
LEVEL PARTIALLY ATTAINED  
REQUEST EXTENDED TIME TO ATTAIN  
LEVEL NOT ATTAINABLE

PORT/CITY Choices (Picklist)

FERNANDINA / ST. MARYS RIVER  
ICW ABOVE JACKSONVILLE  
JACKSONVILLE / ST. JOHNS RIVER DOWNSTREAM BUCKMAN BRIDGE  
ST. JOHNS RIVER UPSTREAM BUCKMAN BRIDGE  
ICW JACKSONVILLE TO PORT CANAVERAL  
ST. AUGUSTINE / MATANZAS INLET  
PONCE INLET / DAYTONA  
PORT CANAVERAL & INDIAN RIVER / BANANA RIVER / MOSQUITO LAGOON  
ICW SOUTH OF PORT CANAVERAL

ENTITY TYPE Choices (Picklist)

VESSEL  
FACILITY  
COMPANY

ENTITY NAME (free text)

DATE (free text)

TIME (free text)

In the body of the E-mail:

PHYSICAL ADDRESS or LAT-LON (free text)

EMERGENCY CONTACT PHONE (free text)

VERSION DATE	VER 1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	TAB Q: 9500-1
-----------------	----------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------

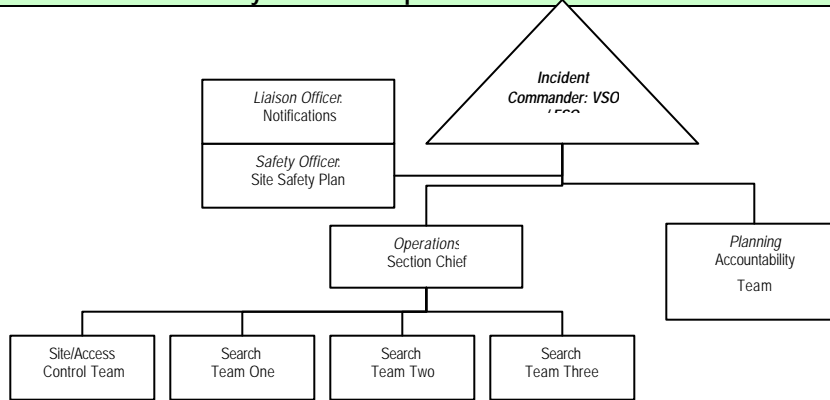


# BOMB THREAT

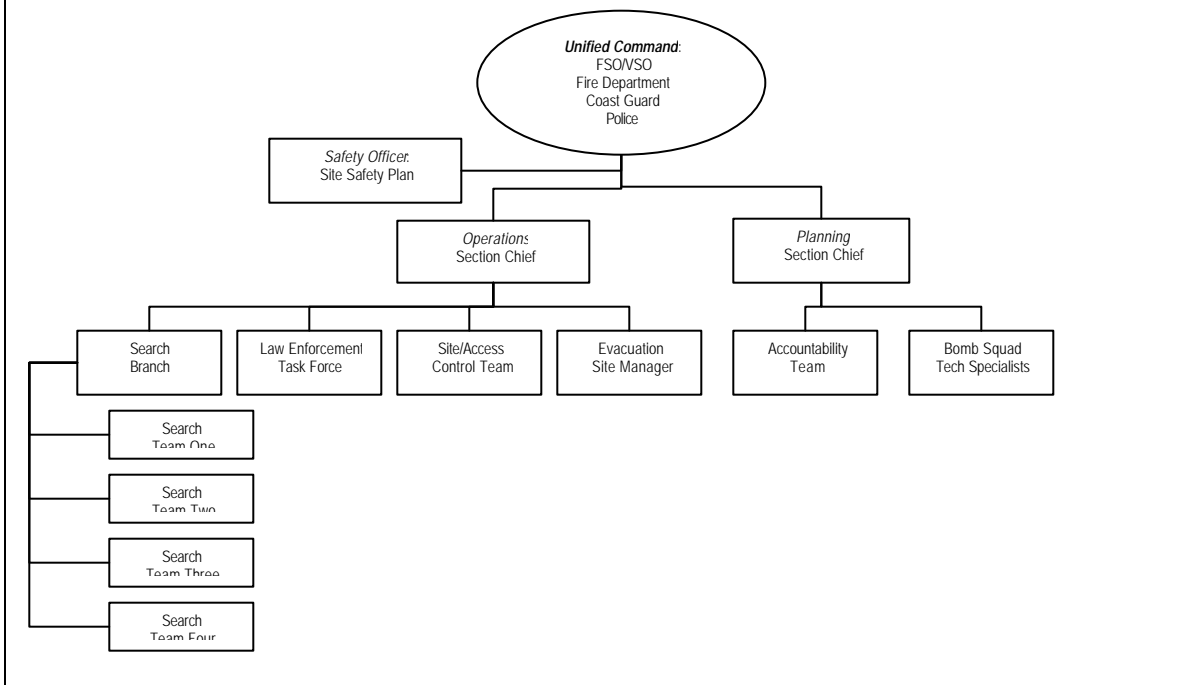
## Immediate Response Actions:

✓	Response Action	Notes
	Using <i>Bomb Threat Checklist</i> (see attached), obtain as much information as possible.	<b>Police &amp; Fire 911</b>  <b>USCG 904-247-7318</b>  <b>FBI Jacksonville</b> 904-721-1211  <b>FBI Orlando</b> 321-752-6021  <b>State Warning Point</b> 800-320-0519  <b>Search Markings:</b>  <i>When you enter:</i>  <i>When you exit:</i>  <b>Floor &amp; Main Entrance:</b> Date and Time your Team LEFT Your search Team's name 1-23-04 1400 hrs Dispatch Team 0 injured 0 dead Any injured Or dead your Team finds Electrical No IED Any hazards Your team finds
	Consider stopping transfers and transits.	
	Notify local Coast Guard; local law enforcement; and the Federal Bureau of Investigation (FBI).	
	If threat is aboard a vessel, maintain communications, and report changes in situation.	
	Prevent unauthorized personnel or vehicles access to the scene.	
	Activate vessel's or facility's bomb threat plan and follow standard operating procedures.	
	Designate command post for responding agencies to report to.	
	Refer to <i>TSI-3 Incident Response Procedures: Explosive Device Discovery</i> if a device is discovered.	
	<b>Bomb Search SOP's:</b> <ul style="list-style-type: none"> <li>- Facility/vessel is responsible for conducting a bomb search since they are more familiar with area than law enforcement authorities.</li> <li>- Only mission is to search for and report any suspicious objects.</li> <li>- Search teams should work in teams of two.</li> <li>- Do not energize or de-energize any electrical switches or use radios during the search.</li> <li>- Most likely areas for a bomb are in or around machinery, large shrubberies, commercial trash bins, and mailboxes.</li> <li>- Amount of time available should dictate whether search is quick sweep or exhaustive search.</li> <li>- Know results of your threat analysis and rating of threat's chance of occurring.</li> <li>- Each team should have separate search area. Prioritize search areas.</li> <li>- Educate searchers in proper use of special equipment that will be used during search.</li> <li>- Develop communication procedures without radios.</li> <li>- Know how to mark searched or "clean" areas.</li> </ul>	

## Recommended Initial Facility/Vessel Response Structure:



## Recommended Reinforced Unified Response Structure:



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab A 9600 SA1-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------

## Checklist for Telephone Bomb Threats

*Place this sheet under your telephone*

### Questions to ask:

When is the bomb going to explode?  
Where is the bomb right now?  
What does the bomb look like?  
What will cause it to explode?  
Did you place the bomb?  
Why?  
What is your address?  
What is your name?

### Write down exact wording of the threat:

Sex of caller:  
Age:

Race:  
Length of call:

### Number at which call was received:

**Time:**

**Date:**

#### Description of caller's voice:

<input type="checkbox"/> calm	<input type="checkbox"/> nasal
<input type="checkbox"/> angry	<input type="checkbox"/> stutter
<input type="checkbox"/> excited	<input type="checkbox"/> lisp
<input type="checkbox"/> slow	<input type="checkbox"/> raspy
<input type="checkbox"/> rapid	<input type="checkbox"/> deep
<input type="checkbox"/> soft	<input type="checkbox"/> rugged
<input type="checkbox"/> loud	<input type="checkbox"/> clearing throat
<input type="checkbox"/> laughter	<input type="checkbox"/> deep breathing
<input type="checkbox"/> crying	<input type="checkbox"/> cracking voice
<input type="checkbox"/> normal	<input type="checkbox"/> disguised
<input type="checkbox"/> distinct	<input type="checkbox"/> accent
<input type="checkbox"/> slurred	<input type="checkbox"/> familiar
<input type="checkbox"/> whispered	

#### Background noise:

<input type="checkbox"/> street noises	
<input type="checkbox"/> factory machinery	
<input type="checkbox"/> crockery	<input type="checkbox"/> animals
<input type="checkbox"/> voices	<input type="checkbox"/> clear
<input type="checkbox"/> PA system	<input type="checkbox"/> static
<input type="checkbox"/> music	<input type="checkbox"/> local
<input type="checkbox"/> house noises	<input type="checkbox"/> booth
<input type="checkbox"/> long distance	<input type="checkbox"/> motor
<input type="checkbox"/> office machinery	

Other:

If voice is familiar, who did it sound like?

### Threat Language:

<input type="checkbox"/> well spoken (educated)	
<input type="checkbox"/> Incoherent	<input type="checkbox"/> taped
<input type="checkbox"/> foul	<input type="checkbox"/> irrational
<input type="checkbox"/> message read by threat maker	

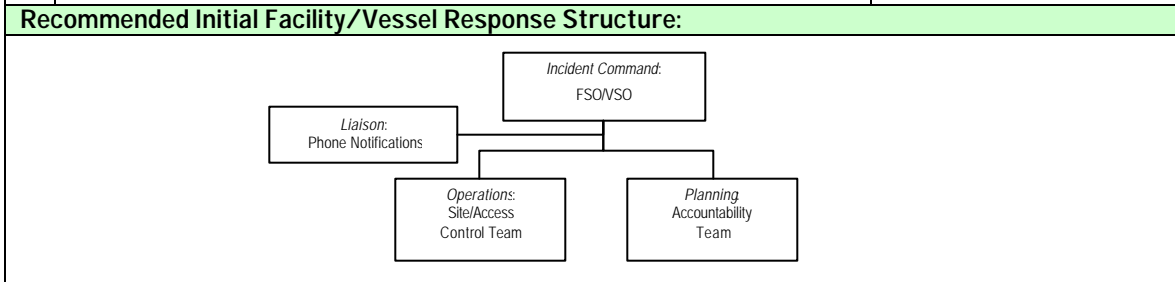
VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab A 9600 SA1-3
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------

## BOMB THREAT

***Write down any other important information about the call on the reverse of this sheet and immediately report incident to law enforcement personnel. This checklist is based on the FBI Bomb Data Center Bomb Threat Checklist***

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab A 9600 SA1-4
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------

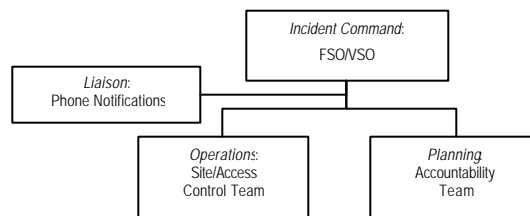
Immediate Response Actions:		
✓	Response Action	Notes
	Make thorough initial report of situation including as many details as possible about personnel, vehicles, actions, and any information regarding the incident. <b><i>Notify the Coast Guard Integrated Command Center immediately.</i></b>	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>Do not use VHF Radio!</b> <b>NRC 800-424-8802</b> <b>Duval Co. Health Dept</b> 904-630-3300 <b>Brevard Co. Health Dept</b> 321-454-7131 <b>BCBP Jacksonville</b> 904-360-5021 <b>BCBP Canaveral</b> 321-783-2066 <b>State Warning Point</b> 800-320-0519 <b>ICE Jacksonville</b> 904-232-2611 <b>ICE Canaveral</b> 321-452-3700 <b>FDLE Jacksonville</b> 1-850-410-7000
	Take photographs of persons attempting delivery of unsolicited/ unexpected packages, persons attempting illegal access (through gates or in vehicles), and unidentified dive operations. All three should be considered illegal trespass attempts until reasonably certain the attempt was innocent.	
	Call 911 if the person, boaters, or divers become belligerent or force entry in any way.	
	Call facility or vessel security officer to verify that a particular activity or operation is supposed to be occurring, e.g., divers doing repair work, personnel repairing fences, pipelines, etc. Update authorities if the activity turns out to be legitimate.	
	Maintain communications with the Coast Guard and report changes in situation.	
	<b><i>This may not have been the first attempted illegal access!</i></b> Activate the Facility or Vessel Security Plan and conduct a search of facility or vessel for trespassing persons, explosive devices, signs of tampering, and suspicious packages possibly including poisons, gasses or hazardous material.	



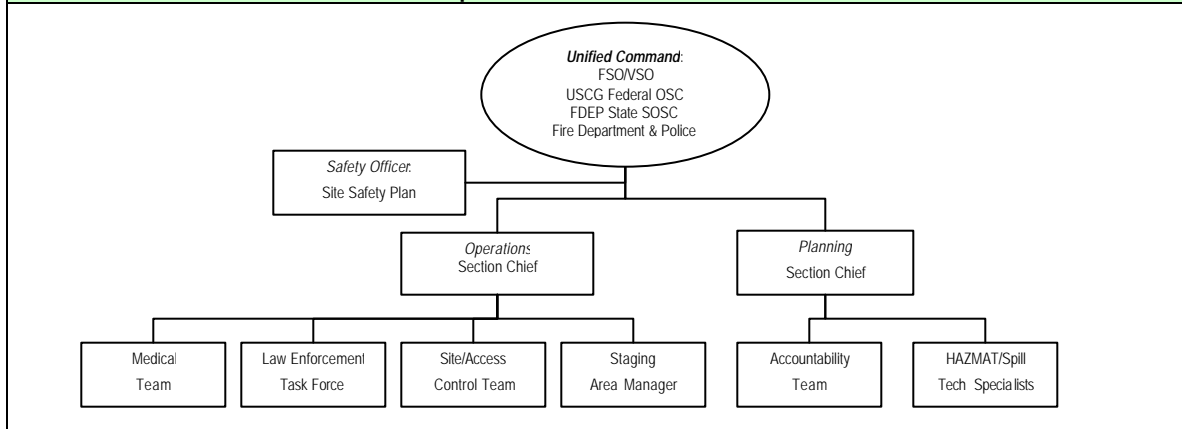
## Immediate Response Actions:

✓	Response Action	Notes
	Make thorough initial report of situation including as many details as possible about personnel, vehicles, actions, and any information regarding the incident. <b><i>Notify the Coast Guard Integrated Command Center immediately.</i></b>	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>Do not use VHF Radio!</b> <b>NRC 800-424-8802</b> <b>Duval Co. Health Dept</b> <b>904-630-3300</b> <b>Brevard Co. Health Dept</b> <b>321-454-7131</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b> <b>ICE Jacksonville</b> <b>904-232-2611</b> <b>ICE Canaveral</b> <b>321-452-3700</b> <b>FDLE Jacksonville</b> <b>1-850-410-7000</b>
	Take photographs of: <ul style="list-style-type: none"> <li>loitering vehicles and vessels, especially small boats;</li> <li>persons taking pictures of facilities, vessels, or infrastructure; persons establishing an unusual business or roadside stand near facilities or infrastructure; and</li> <li>persons soliciting information about vessels, facilities, from;</li> </ul> All three should be considered suspicious activity until reasonably credible explanations can be obtained.	
	Do not approach suspicious persons, vehicles, or boats without due consideration for security personnel safety! Ask authorities if you should approach the person before they arrive – do not drive the person away! If approach appears safe and prudent, ask the person for as much information as possible and be alert for signs of belligerence or evasiveness.	
	Collect detailed statements about: <ul style="list-style-type: none"> <li>Persons calling facilities to learn security procedures;</li> <li>Persons attempting to learn about facility or vessel security measures from employees or their families; and</li> <li>Employees acting outside the scope of duties, loitering in unusual areas.</li> </ul> All three should be considered suspicious activity until reasonably credible explanations can be obtained.	
	Activate your vessel/facility security plan regarding Operational Security and institute changes in your operational signals to confuse/deter persons trying to determine your routine through surveillance.	
	Call facility or vessel security officer to see if the particular activity might be legitimate (even if unusual). Update authorities if the activity turns out to be legitimate.	
	Distribute look-out information to all facility and vessel security personnel so they can recognize the suspicious person, vehicle, or boat. Call the Coast Guard if the suspicious person, vehicle, or boaters return to the facility or vessel.	
	Maintain communications with the Coast Guard and report changes in situation.	
	<b><i>This may not be an isolated event!</i></b> Activate the Facility or Vessel Security Plan and conduct a search of facility or vessel for trespassing persons, explosive devices, signs of tampering, and suspicious packages possibly including poisons, gasses or hazardous material.	

## Recommended Initial Facility/Vessel Response Structure:



**Recommended Reinforced Unified Response Structure:**



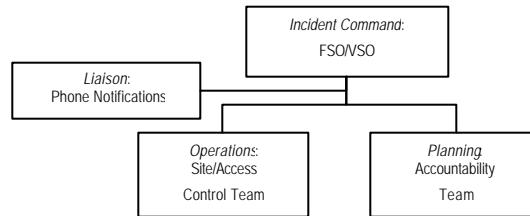
VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab A SA3 9600-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------



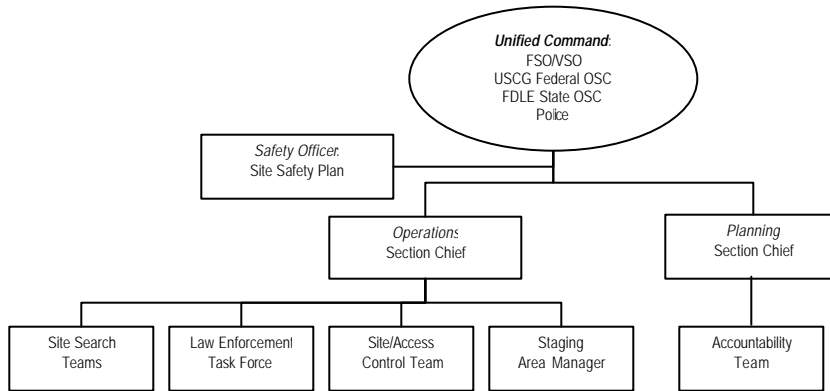
# TRESPASS & STOWAWAY

Immediate Response Actions:		
✓	Response Action	Notes
	<p>Use discretion in approaching trespassers or stowaways; their intentions should not be assumed as harmless or unarmed.</p> <p><input type="checkbox"/> If the person reasonably appears to be a trespasser and can be safely approached, confront the person and challenge the person's right to access the vessel or facility. Collect as much information as possible.</p> <p><input type="checkbox"/> If the person reasonably appears to be a stowaway and can be safely approached, confront the person and inform them that fleeing the scene may be interpreted by law enforcement as a crime.</p> <p><input type="checkbox"/> If the person cannot be reasonably approached, or if the person runs/becomes hostile when approached, treat the person as an armed intruder and <b>respond accordingly! See TSI-4, Response Procedures for Armed Trespass.</b> Maintain awareness of the individual's location to the maximum extent possible, but do not attempt citizens arrest or similar unless your personnel have been trained and equipped to do so. Immediately call <b>911</b>.</p>	<p><b>Police &amp; Fire 911</b></p> <p><b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b></p> <p><b>BCBP Jacksonville</b> 904-360-5021 <b>BCBP Canaveral</b> 321-783-2066</p> <p><b>State Warning Point</b> 800-320-0519</p> <p><b>ICE Jacksonville</b> 904-232-2611 <b>ICE Canaveral</b> 321-452-3700</p> <p><b>FBI Jacksonville</b> 904-721-1211 <b>FBI Orlando</b> 321-752-6021</p>
	Stowaways who leave a vessel should be considered fugitives, not trespassers – alert local police by dialing <b>911</b> immediately. Tell the police that the incident involves illegal immigrants for clarity.	
	Simple, unintentional trespass is not typically an offense for which local police will arrest or detain. Nevertheless, <b>without losing sight of the person or accountability for their whereabouts</b> , alert local police that a validated trespass is ongoing immediately.	
	Designate command post for responding agencies to report to.	
	<b>Without losing sight of the person or accountability for their whereabouts</b> , notify the National Response Center, the Coast Guard Integrated Command Center, and Customs and Border Protection. You are required by federal regulations at 33 CFR part 101.305(b) to report to the NRC because (regardless of intent) stowaways and trespassers constitute a breach of security.	
	Take photographs of trespassers and/or stowaways.	
	When the trespasser / stowaway presents a reasonable explanation of their presence, call facility or vessel security officer to verify the person's presence is legitimate. Update authorities if the activity turns out to be legitimate. If the person admits to trespass and/or stowing away, document the details as much as possible, <b>particularly ask about other trespassers or stowaways – do not assume the person is acting alone!</b>	
	Consider stopping transfers and transits.	
	Maintain communications with the Coast Guard and report changes in situation.	
	<b><i>This may not have been the first attempted illegal access!</i></b> Activate the Facility or Vessel Security Plan and conduct a search of facility or vessel for other trespassing persons, explosive devices, signs of tampering, and suspicious packages possibly including poisons, gasses or hazardous material. Additional security breaches must be separately reported to authorities – do not consider them “covered” by the earlier notification.	

## Recommended Initial Facility/Vessel Response Structure:



## Recommended Reinforced Unified Response Structure:



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab B 9600 SB1-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------

## SMALL ILLEGAL PROTEST

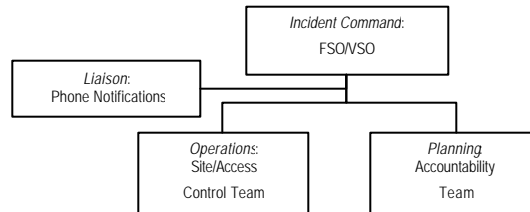
Immediate Response Actions:		
✓	Response Action	Notes
	<p>Many shore-side small gatherings are legal without authorization from local government, and local government without general public knowledge legally permits many small gatherings. Do not assume that small protest gatherings are illegal by their nature. Remember that peaceable protests are constitutionally protected free speech.</p> <p><input type="checkbox"/> Estimate the number of people and note the general actions they are taking (blocking roads, staging a “sit in,” peaceable or violent).</p> <p><input type="checkbox"/> Contact the police at 911 to inquire about the small gathering. The police will inform you whether the event is legal and/or permitted.</p>	<p><b>Police &amp; Fire 911</b></p> <p><b>USCG 904-247-7318</b></p> <p><b>FBI Jacksonville</b> 904-721-1211</p> <p><b>FBI Orlando</b> 321-752-6021</p> <p><b>State Warning Point</b> 800-320-0519</p>
	<p>Any waterborne gathering (including canoes and kayaks) blocking or impinging upon the navigable waterway must have a permit issued by the Coast Guard. Remember that peaceable protests are constitutionally protected free speech.</p> <p><input type="checkbox"/> Estimate the number of people and vessels and note the general actions they are taking (blocking the channel, peaceable, or violent).</p> <p><input type="checkbox"/> Immediately inquire about these gatherings by hailing the Coast Guard on VHF Channel 16. The Coast Guard will inform you whether a permitted marine event is authorized at your location.</p>	
	While protests are legal, there is a danger that they may escalate to include violence. Activate the Facility or Vessel Security Plan, inform the VSO/FSO and CSO, and pass the word to all employees.	
	Secure and lock gates, etc., including internal gates; raise pilot ladders, and minimize ease of access thru vessel.	
	Employees (including those on the weather deck aboard ship) readily visible to the protest area may become targets and should be aware of thrown objects – consider moving these personnel from sight.	
	Employee vehicles, etc., inside a facility protected by fencing from the protest area may become targets for thrown objects. If these vehicles can be relocated outside the range of thrown objects without inflaming the protest, consider moving them from sight.	
	The illegal protest becomes a security breach for a vessel or a facility when protestors successfully force entry onto the ship or the facility itself (essentially a “mass intrusion”). Security personnel are not usually trained or equipped for civil disorder operations, and attempts to do so for those seeking simple arrest for civil disobedience are counter-productive and may escalate the situation into violence. Immediately report to <b>911</b> , the <b>NRC</b> , and the Coast Guard Integrated Command Center if a mass intrusion is about to occur or occurs suddenly.	
	Consider stopping transfers and transits, maintain the navigational safety of your vessel, and consider diverting arriving traffic for terminals and facilities.	
	Where the situation allows, approach the protestors. Carefully inform them that their intrusion is illegal trespass, but explain that the vessel/facility does not wish the protest to become violent. Explain that the facility/vessel is an industrial location and that dangers exist, not all areas are suitable for civil disobedience. Try to establish a perimeter within the facility where the civil disobedience can be safely executed, then maintain security personnel at that perimeter. Remind the protestors that it is the vessel or facilities wish that they depart entirely, but if they are intent on civil disobedience, they must remain within the perimeter for their own safety.	

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab B 9600 SB2-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------

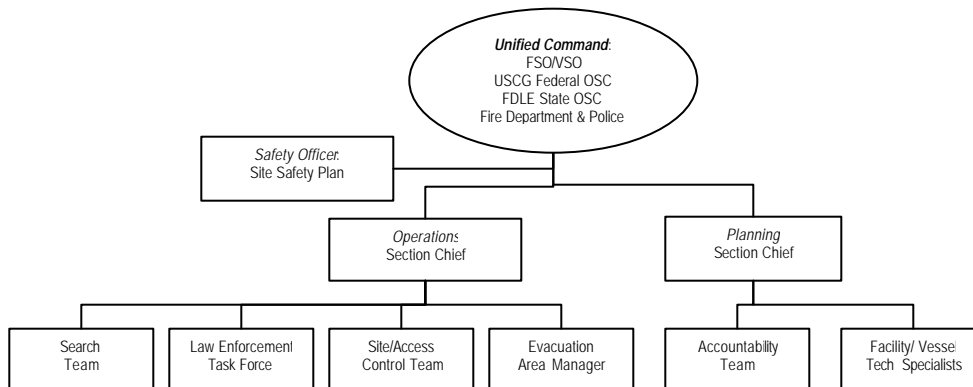
## SMALL ILLEGAL PROTEST

	<b>Without exposing personnel to danger from violent protest or thrown objects, maintain accountability for protestor whereabouts.</b> Maintain communications with the Coast Guard and report changes in situation.	
	<b><i>This may not be the only attempt to intrude onto the facility or vessel!</i></b> Increase your surveillance and scrutiny of all vessel and facility access points and perimeters, particularly the waterside. Illegal protestors typically attempt more than a single means of access.	
	<b><i>This may not have been the first attempted illegal activity! Consider the possibility that the protest is a diversionary activity preceding a violent or terrorist act.</i></b> Activate the Facility or Vessel Security Plan and conduct a search of facility or vessel for other trespassing persons, explosive devices, signs of tampering, and suspicious packages possibly including poisons, gasses or hazardous material. Additional security breaches must be separately reported to authorities – do not consider them “covered” by the earlier notification.	
	Prepare to execute the facility / vessel evacuation procedures in the event of a discovered device, violent attack, or simple “overrunning” of the facility by protestors. Consider alternate evacuation routes (because of the protest), and remember to search rally points for planted IEDs before allowing people to meet there!	

### Recommended Initial Facility/Vessel Response Structure:



### Recommended Reinforced Unified Response Structure:



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab B 9600 SB2-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	------------------------

## SECURITY SYSTEM TAMPERING

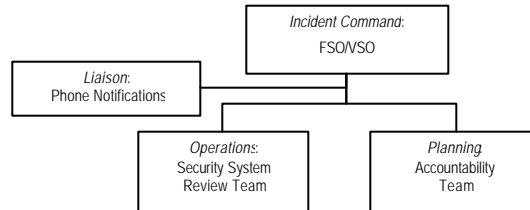
Immediate Response Actions:		
✓	Response Action	Notes
	<b>Security System</b> means any device, or multiple devices, designed, installed, and operated to monitor, detect, observe, or communicate about activity that may pose a security threat in a location or locations on a vessel or facility. For the purposes of this procedure, fences, barriers, walls, and other delaying devices forming part of an intruder deterrence/detection system are part of such a security system.	Police & Fire 911  USCG 904-247-7318  NRC 800-424-8802
	Monitor the status of your vessel and facility security systems on a routine, recurring basis. Develop attention checks for security personnel assuring that security systems are monitored, not assumed unchanged since last periodic monitor.	FBI Jacksonville 904-721-1211  FBI Orlando 321-752-6021
	When evidence of tampering is discovered, note the specific form of tampering: <input type="checkbox"/> <b>Deactivated mechanical, electrical, or electronic systems</b> (e.g., deactivated communication or alarm systems, computers turned off, fuses pulled, lights de-energized, etc.). <input type="checkbox"/> <b>Blocked/neutralized systems</b> (e.g., cameras redirected, gangways or access-points unattended, cameras spray-painted, ladders leaning against fences, ropes hanging down over docks, sensors re-located, external power supply disrupted, holes dug under fencing, transponders removed or relocated, etc.). <input type="checkbox"/> <b>Damaged systems</b> (e.g., holes cut in fences, cameras smashed, lights shot out; locks jimmied, radios broken, phone-lines cut, doors kicked open; signs and warnings removed or defaced, etc.) <input type="checkbox"/> <b>Improper Records and systems</b> access (e.g., training files clearly accessed without explanation, computers left open for access, unexplained internal e-mail or message traffic, hacking into security sensitive computer files from within or outside the company, etc.).	State Warning Point 800-320-0519
	Contact the VSO/FSO and CSO, ensure that the noted evidence of tampering is not readily explained by un-announced system maintenance or other authorized activity. NOTE: Do not be quick to assume records access is simply employee error: inform the authorities <i>just in case</i> . They can be updated with the error in reporting at a later time after you've conclusively identified the problem as simple employee error.	
	Where the system has been tampered with or the situation is unclear, <b>notify the NRC and the Coast Guard ICC</b> (regardless of the tampering type).	
	Where the type of tampering includes physical damage or could only be accomplished by trespassing, call the local police at <b>911</b> .	
	Where the type of tampering involves possible computer crime (especially hacking from outside), notify and consult the Federal Bureau of Investigation.	
	<b><i>This may not have been the only illegal access!</i></b> Activate the Facility or Vessel Security Plan and conduct a search of facility or vessel for other trespassing persons, explosive devices, signs of tampering, and suspicious packages possibly including poisons, gasses or hazardous material. Additional security breaches must be separately reported to authorities – do not consider them “covered” by the earlier notification.	

# SECURITY SYSTEM TAMPERING

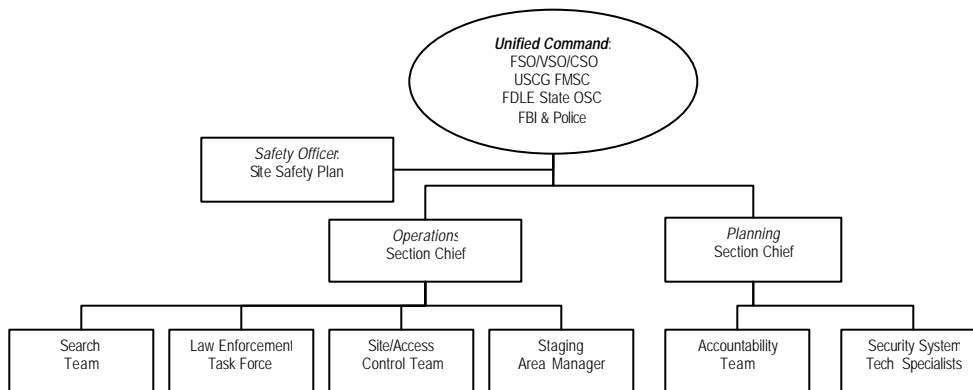
Consider the possibilities for re-activating and/or implementing alternative temporary security measures that would restore the security of the vessel and/or facility. Report to the Coast Guard Integrated Command Center which temporary measures are in place and how long it will be until permanent repair/restoration is accomplished. Consult police and FBI in establishing both so as to avoid contaminating the crime scene for possible criminal prosecution purposes.

Maintain communications with the Coast Guard and report changes in situation.

## Recommended Initial Facility/Vessel Response Structure:



## Recommended Reinforced Unified Response Structure:



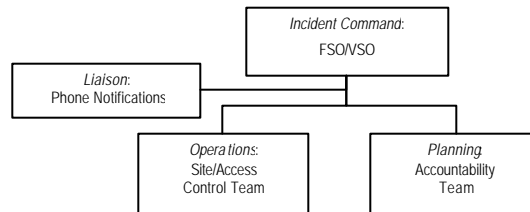
Immediate Response Actions:		
✓	Response Action	Notes
	Under federal regulations, any facility or property located on or adjacent to navigable waters of the United States, including those not required have their own federally-approved facility security plan, must implement the security measures specified in the Area Maritime Security Plan (see 33 CFR part 105.105(b)). The same is true for security measures aboard all vessels (see 33 CFR part 104.105(b)).	<b>Police &amp; Fire 911</b>  <b>USCG 904-247-7318</b>  <b>NRC 800-424-8802</b>  <b>State Warning Point</b> 800-320-0519  <b>BCBP Jacksonville</b> 904-360-5021  <b>BCBP Canaveral</b> 321-783-2066
	Facilities with federally-approved Facility Security Plans must implement the security measures in their FSPs for the appropriate security condition. See 33 CFR 105.115(b). The same is true for vessels with federally-approved Vessel Security Plans; see 33 CFR 104.115. Foreign vessels must comply with the International Ship and Port Facility (ISPS) code including an approved vessel security plan; see 33 CFR 115(c). These vessel and facility security measures are in addition to the security measures outlined in the Area Maritime Security Plan	
	Establish a system for periodically and routinely checking your property, facility, or vessel implementation of all Security Measures. For facilities and vessels with approved security plans, the Vessel or Facility Security Officer <b>must</b> regularly inspect the vessel [or facility] to ensure that security measures are maintained. See 33 CFR 104.215(c)(1) and 33 CFR 105.205(c)(5).	
	Any security measure established by the Area Maritime Security Plan, a Vessel Security Plan, or a Facility Security Plan found not to be in place is a security breach. If a security measure is not in place: <input type="checkbox"/> Call the NRC immediately. <input type="checkbox"/> Notify the Coast Guard Integrated Command Center <input type="checkbox"/> Where there is evidence the security measure was not in place due to a crime, report the incident immediately to the local police at <b>911</b> . <input type="checkbox"/> Where the breach occurs on port-authority owned property within the State of Florida, call the relevant Port Authority Security Director and the Florida Department of Law Enforcement. <input type="checkbox"/> Where the measure not in place affects foreign crewmen, a Customs Zone, or cargo security, call the Customs and Border Protection office.	
	<b><i>This may not be the only issue!</i></b> Activate the Facility or Vessel Security Plan and conduct a search of facility or vessel for trespassing persons, explosive devices, signs of tampering, and suspicious packages possibly including poisons, gasses or hazardous material. Additional security breaches must be separately reported to authorities – do not consider them “covered” by the earlier notification. Scope the extent to which your vessel or facility may have been compromised by the lack of the security measure. Validate all your other security measures are still in place.	
	Establish a firm recording process for information you develop about the lack of the security measure being in place: <input type="checkbox"/> When, where, how was the lack of a measure discovered? <input type="checkbox"/> Why was the measure not in place? Are all other measures in place? <input type="checkbox"/> How long was the measure not in place? <input type="checkbox"/> What did you do to scope the extent of possible compromise at the facility and vessel? What were the results?	



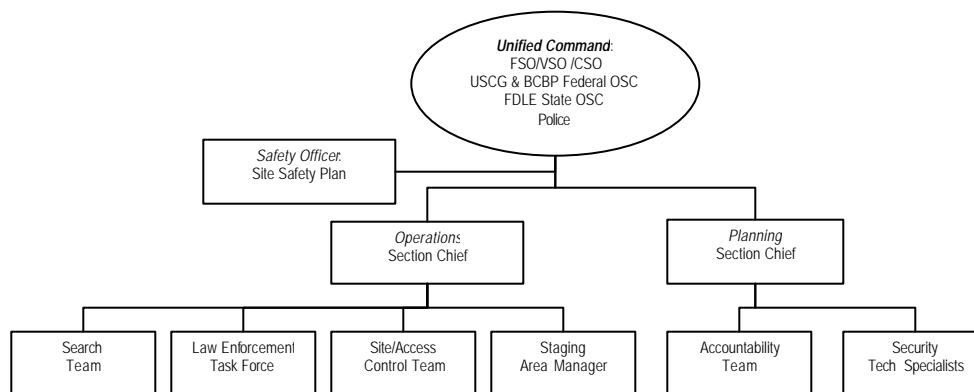
Consider the possibilities for re-activating and/or implementing alternative temporary security measures that would restore the security of the vessel and/or facility. Report to the Coast Guard Integrated Command System which temporary measures are in place and how long it will be until permanent repair/restoration is accomplished. Consult police and FBI in establishing both so as to avoid contaminating the crime scene for possible criminal prosecution purposes.

Maintain communications with the Coast Guard and report changes in situation.

**Recommended Initial Facility/Vessel Response Structure:**



**Recommended Reinforced Unified Response Structure:**



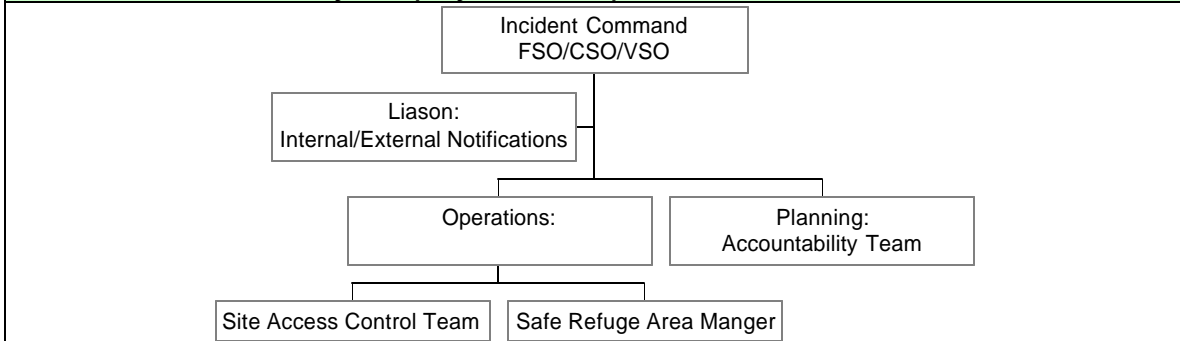
Area Maritime Security Plan Incident Response Procedures TSI-1 UNCLASSIFIED – All Port Entities	ROGUE/HIJACKED VESSEL
---	-----------------------

Immediate Response Actions:		
✓	Response Action for Facility, Company or Moored Vessel	Notifications
	<b>If receiving report of Rogue Vessel:</b> Perform below response actions as appropriate. Record at a minimum the following information: <b>Time of Notification/Estimated time to Rogue arrival</b>	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>VHF Channel 16/22A</b> <b>NRC 800-424-8802</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b> <b>ICE Jacksonville</b> <b>904-232-2611</b> <b>ICE Canaveral</b> <b>321-452-3700</b>
	<b>If reporting Rogue Vessel:</b> Perform below response actions as appropriate. Perform Initial Assessment noting vessel location, name, type, direction and estimated speed.	
	Notify US Coast Guard providing initial assessment information. Maintain communications link with US Coast Guard.	
	If possible, monitor and report the status/movements of the Rogue Vessel.	
	Notify agencies listed in “Notifications” column, providing initial assessment information.	
	Notify/Communicate the initial assessment/report of Rogue Vessel to facility/company/vessel security officer, as appropriate.	
	Activate facility/vessel security plans and notify adjacent facilities/companies/vessels.	
	Secure all passenger, cargo and bunker operations at the facility/company/vessel.	
	Evacuate all non-essential facility/company/vessel personnel to emergency shelter.	
	If possible, remove flammable, explosive and hazardous material from facility waterfront and pier area.	
	Evacuate all remaining personnel from waterfront and pier areas to emergency shelter.	
	Secure emergency lighting and power to the pier and waterfront areas.	
	Determine the need for additional personal protective measures.	
	Select and communicate the incident command post location.	
	Establish incident command (ICS or Unified) structure.	
	Develop Incident Objectives and Incident Action Plan.	
	Request appropriate staffing and equipment.	
	Perform traffic control, crowd control and force protection functions.	

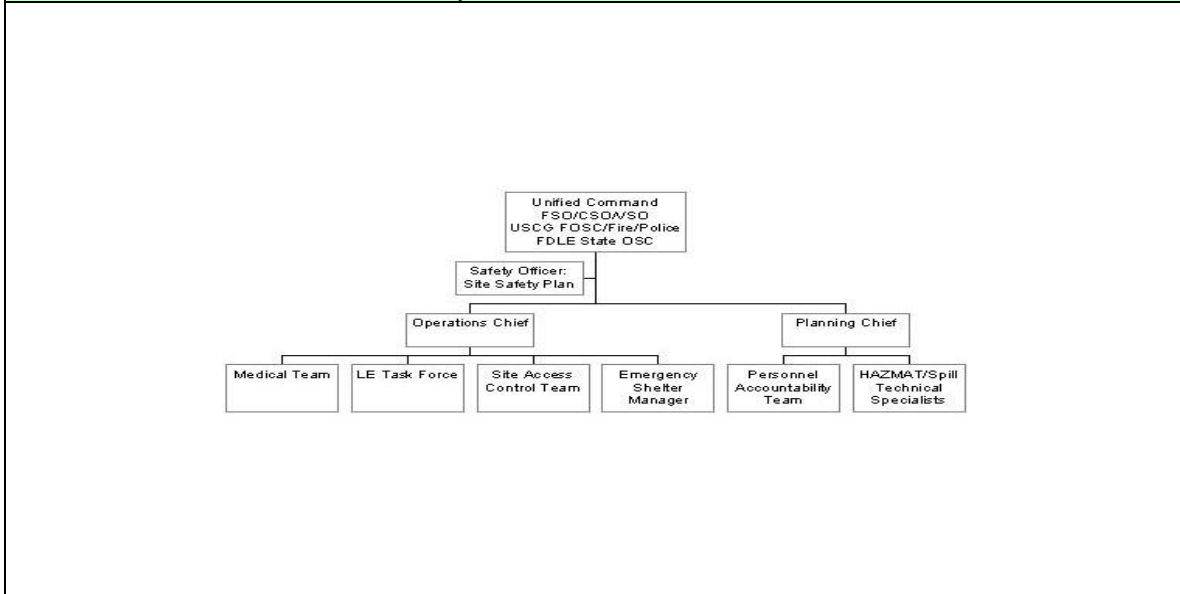
✓	Response Action for Vessel Underway within Port Limits	Notifications
	Notify US Coast Guard and Company/Vessel Security Officer.	<b>USCG</b> <b>904-247-7318</b> <b>VHF Channel 16/22A</b>
	Slow to bare steerageway.	
	Activate vessel security plan.	
	Await specific instructions regarding vessel movement from the US Coast Guard Integrated Command Center (ICC) on VHF Channel 16 and/or 22A.	
	Do not allow any other vessels to approach unless directed by US Coast Guard.	
	Do not allow any personnel to board or debark the vessel unless directed by Coast Guard.	

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 1 -1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

**Recommended Initial Facility/Company/Vessel Response Structure:**



**Recommended Reinforced Unified Response Structure:**

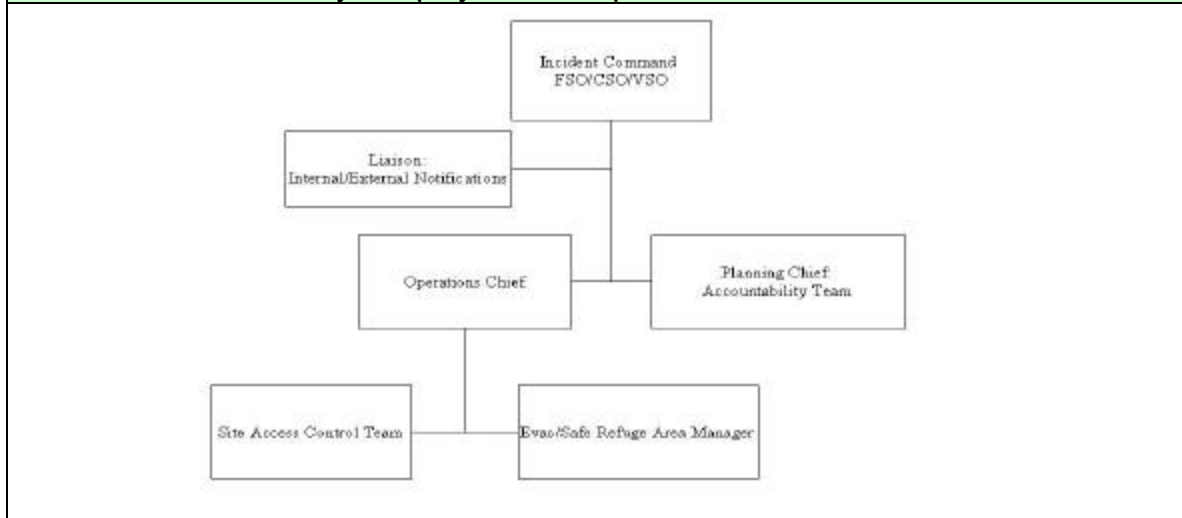


# CHEM-BIO-RADIOLOGICAL TERRORISM

Immediate Response Actions:		
✓	Response Action for Facility, Company or Moored Vessel	Notifications
	<b><u>Every incidence or report of intentional release of toxic chemicals, suspicious disease outbreak, unexplained casualties, and radiological monitoring equipment alarms should be presumed terrorism until ruled out.</u></b>	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b> <b>CDC 888-246-2675</b> 8am-11pm MF 10am-9pm SS <b>Nassau Co. Health Dept</b> 904-277-7287 <b>Duval Co. Health Dept</b> 904-630-3300 <b>Brevard Co. Health Dept</b> 321-454-7131 <b>BCBP Jacksonville</b> 904-360-5021 <b>BCBP Canaveral</b> 321-783-2066 <b>State Warning Point</b> 800-320-0519 <b>ICE Jacksonville</b> 904-232-2611 <b>ICE Canaveral</b> 321-452-3700 <b>DOE Region 3 RAP</b> 803-952-6613
	Conduct Initial Assessment of the situation, noting location and size of affected area, number and type of casualties, description of possible contaminate special hazards and assistance required.	
	Notify/Communicate the initial assessment to Facility/Company/Vessel security officer, as appropriate.	
	Activate facility/vessel security plans and notify adjacent facilities/vessels.	
	Provide direction to first responders.	
	Establish containment. Preserve the scene, inner/outer perimeter and zones of operation.	
	Determine the need for immediate personal protective measures.	
	If applicable, secure ventilation systems.	
	Evacuate personnel from immediate area of affected area to emergency shelter or provide in-place protection.	
	Quarantine all personnel evacuated to emergency shelter and any personnel suspected of coming into contact with affected areas or personnel.	
	Do not allow unauthorized movements into or out of affected area or emergency shelter.	
	Select and communicate the incident command post location.	
	Establish incident command (ICS or Unified) structure.	
	Develop Incident Objectives and Incident Action Plan.	
	Request appropriate staffing and equipment.	
	Perform traffic control, crowd control and force protection functions.	
	Notify agencies listed in "Notifications" column, providing initial assessment information.	
	Determine all personnel onboard the facility/vessel and do not allow personnel to leave the facility/vessel.	
	Determine all personnel who may have been aboard facility/vessel, and departed, before alarm was raised.	
	Secure all passenger, cargo and bunker operations at the affected facility/company/vessel.	
	Select and equip decontamination area.	
	Monitor all personnel at the facility and vessels moored at the facility (when detected pier-side) for possible contamination contact.	
	Stay upwind, uphill, and upstream from suspected contamination/outbreak source.	

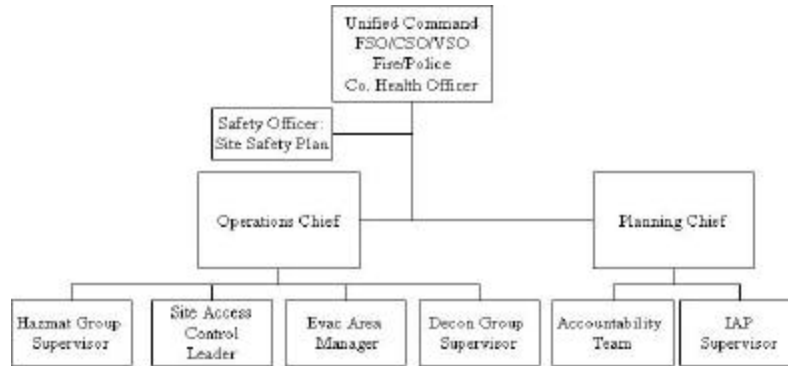
✓	Response Action for Vessel Underway within Port Limits	Notifications
	Notify US Coast Guard and Company/Vessel Security Officer.	<b>USCG</b> 904-247-7318 VHF Channel 16/22A
	Slow to bare steerageway.	
	Activate vessel security plan.	
	If installed, activate SSAS.	
	Await specific instructions regarding vessel movement from the US Coast Guard Integrated Command Center (ICC) on VHF Channel 16 and/or 22A.	
	Do not allow any other vessels to approach unless directed by US Coast Guard.	
	Do not allow any personnel to board or debark the vessel unless directed by Coast Guard.	

## Recommended Initial Facility/Company/Vessel Response Structure:



## Recommended Reinforced Unified Response Structure:

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 2 -2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 2 -3
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

Area Maritime Security Plan Incident Response Procedures TSI-3 UNCLASSIFIED – All Port Entities	<b>EXPLOSIVE/INCENDIARY DEVICE SUSPECTED OR DETECTED</b>
---	--

Response Action for Facility, Company or Moored Vessel		
✓	Response Action	Notifications
	Conduct Initial Assessment of the situation using facility/company/vessel standard bomb threat checklist to gather important information regarding bomb.	<b>Do not use VHF Radio!</b> <b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b> <b>ICE Jacksonville</b> <b>904-232-2611</b> <b>ICE Canaveral</b> <b>321-452-3700</b>
	Notify/Communicate the initial assessment to Facility/Company/Vessel security officer, as appropriate.	
	Activate facility/vessel security plans/bomb incident plans and notify adjacent facilities/vessels.	
	Provide direction to first responders.	
	Establish containment. Preserve the scene, inner/outer perimeter and zones of operation.	
	Determine the need for immediate personal protective measures.	
	Secure all passenger, cargo and bunker operations at the affected facility/company/vessel.	
	Evacuate personnel from immediate area of affected area to emergency shelter.	
	Do not allow unauthorized movements into or out of affected area or emergency shelter.	
	Select and communicate the incident command post location.	
	Establish incident command (ICS or Unified) structure.	
	Develop Incident Objectives and Incident Action Plan.	
	Request appropriate staffing and equipment.	
	Perform traffic control, crowd control and force protection functions.	
	Notify agencies listed in “Notifications” column, providing initial assessment information.	
	Determine all personnel onboard the facility/vessel and do not allow personnel to leave the facility/vessel.	
	Determine all personnel who may have been aboard facility/vessel, and departed, before alarm was raised.	
	Do not operate equipment, electronics, or radios within 500 feet of bomb.	
	Conduct search of facility and moored vessels for additional explosive devices.	
	Consider emergency departure of vessels moored at facility.	

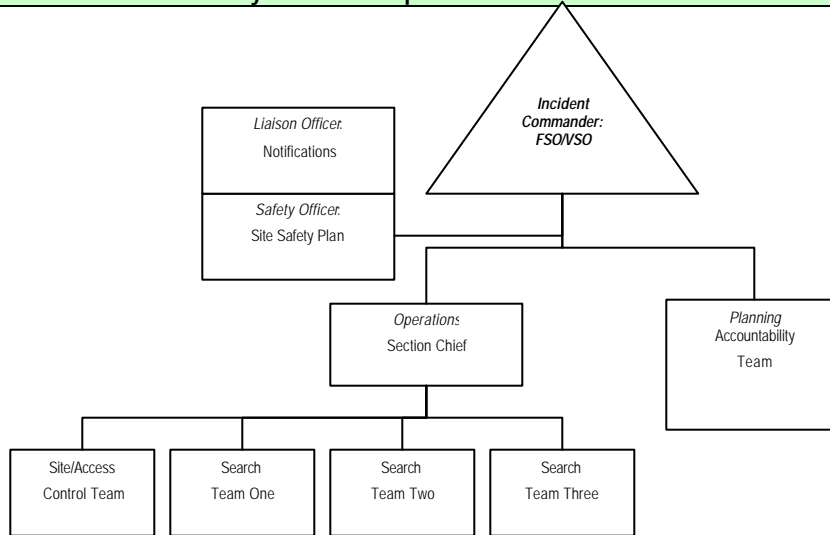
✓	Response Action for Vessel Underway within Port Limits	Notifications
	Notify US Coast Guard and Company/Vessel Security Officer.	<b>Do not use VHF Radio!</b> <b>USCG</b> <b>904-247-7318</b>
	Slow to bare steerageway.	
	Activate vessel security plan.	
	If installed, activate SSAS.	
	Await specific instructions regarding vessel movement from the US Coast Guard Integrated Command Center (ICC) on VHF Channel 16 and/or 22A.	
	Do not allow any other vessels to approach unless directed by US Coast Guard.	
	Do not allow any personnel to board or debark the vessel unless directed by Coast Guard.	

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 3 -1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

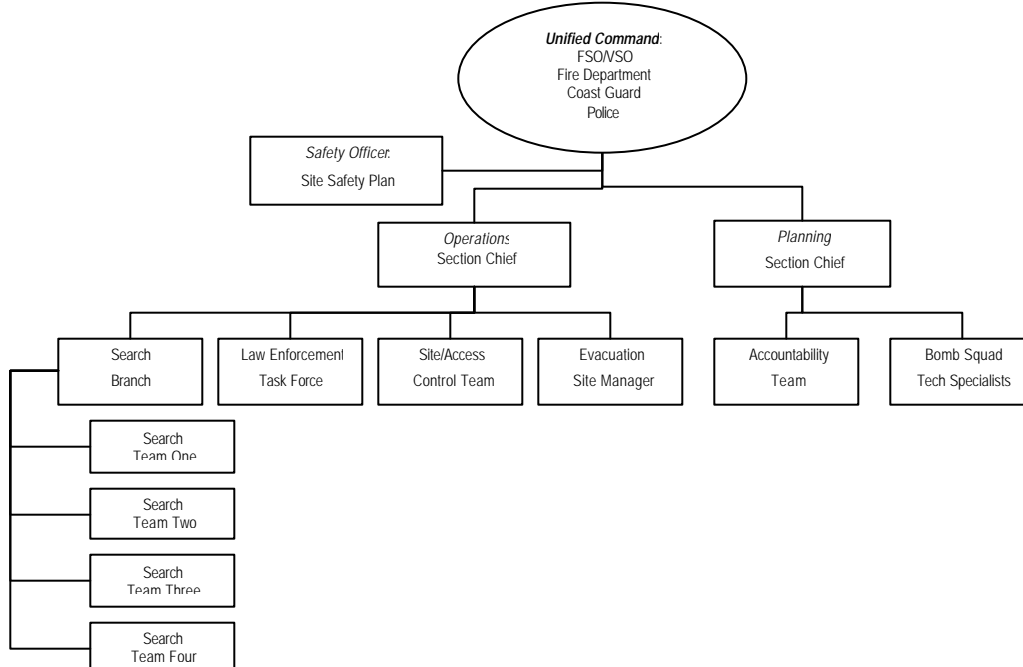


# EXPLOSIVE/INCENDIARY DEVICE SUSPECTED OR DETECTED

## Recommended Initial Facility/Vessel Response Structure:



## Recommended Reinforced Unified Response Structure:

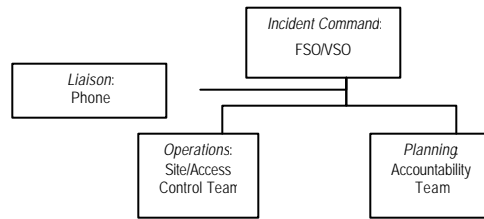


Area Maritime Security Plan Incident Response Procedures TSI-4 UNCLASSIFIED – All Port Entities	<b>ARMED TRESPASS</b>
---	-----------------------

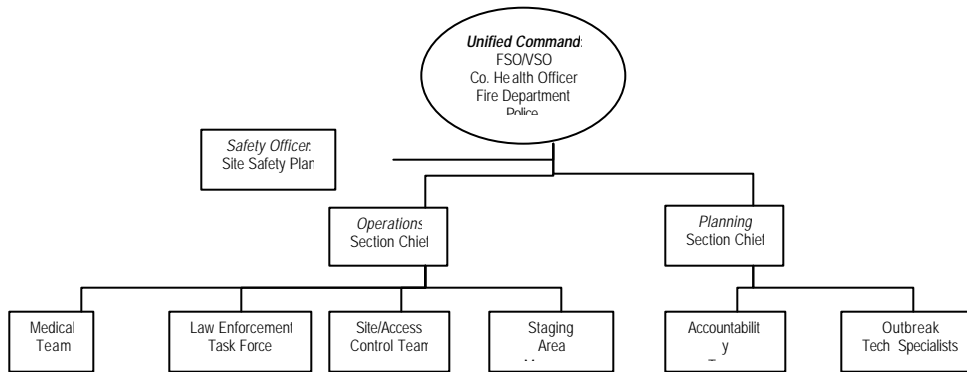
Response Action for Facility, Company or Moored Vessel		
✓	Response Action	Notifications
	Activate facility/company/vessel security alert alarm system.	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b> <b>ICE Jacksonville</b> <b>904-232-2611</b> <b>ICE Canaveral</b> <b>321-452-3700</b>
	Conduct Initial Assessment of the situation to gather important information regarding incident.	
	Notify/Communicate the initial assessment to Facility/Company/Vessel security officer, as appropriate.	
	Activate facility/company/vessel security plans and notify adjacent facilities/vessels.	
	Provide direction to first responders.	
	Establish containment. Preserve the scene, inner/outer perimeter and zones of operation.	
	Determine the need for immediate personal protective measures.	
	Secure all passenger, cargo and bunker operations at the affected facility/company/vessel.	
	Evacuate personnel from immediate area of affected area to emergency shelter.	
	Do not allow unauthorized movements into or out of affected area or emergency shelter.	
	Select and communicate the incident command post location.	
	Establish incident command (ICS or Unified) structure.	
	Develop Incident Objectives and Incident Action Plan.	
	Request appropriate staffing and equipment.	
	Perform traffic control, crowd control and force protection functions.	
	Notify agencies listed in “Notifications” column, providing initial assessment information.	
	Consider emergency departure of vessels moored at facility.	

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 4 -1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

## Recommended Initial Facility/Vessel Response Structure:



## Recommended Reinforced Unified Response Structure:

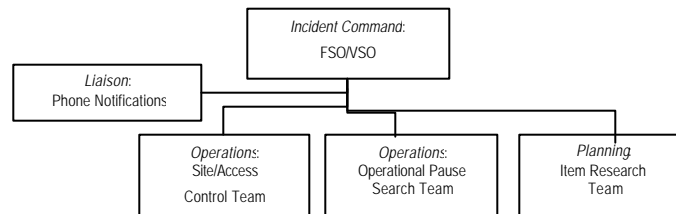


# SUSPECT CARGO/ITEM

## Immediate Response Actions:

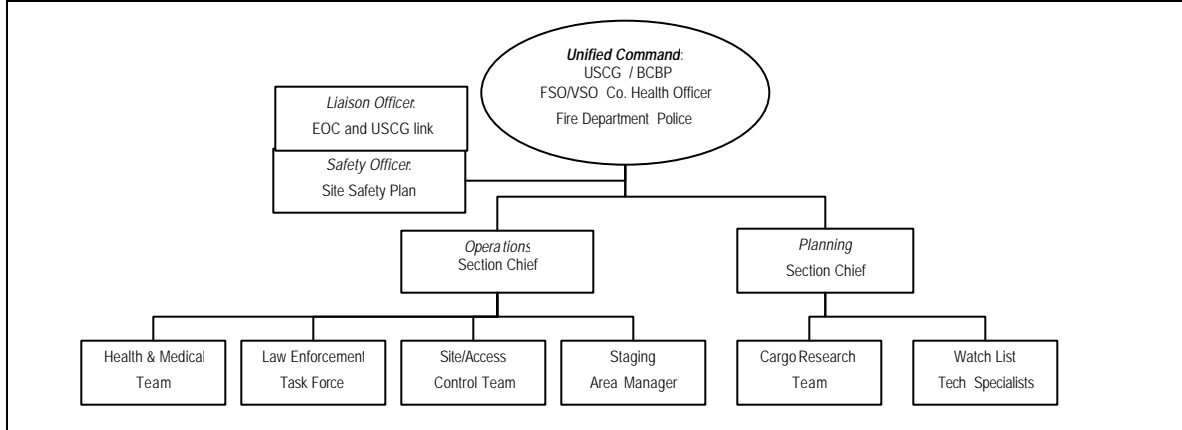
✓	Response Action	Notes
	<p>Check for substances, devices, and equipment on the <b>Suspect Item Watch List</b> (attached) during all security and safety screening activity.</p> <p><input type="checkbox"/> When you detect an object apparently on the <b>Watch List</b>, obtain cargo or shipping information that may clearly indicate the object is <b>NOT</b> on the <b>Watch List</b> (e.g., a piece of equipment is an Air Conditioning pump, not a <b>Watch List</b> pressure vessel).</p> <p><input type="checkbox"/> If the object has been proven <b>NOT</b> on the <b>Watch List</b>, make security entries to that effect; <b>otherwise</b> proceed with this TSI Response Procedure!</p>	<p><b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>Do not use VHF Radio!</b> <b>NRC 800-424-8802</b> <b>CDC 888-246-2675</b> 8am-11pm MF 10am-9pm S-S <b>Duval Co. Health Dept</b> 904-630-3300 <b>Brevard Co. Health Dept</b> 321-454-7131 <b>BCBP Jacksonville</b> 904-360-5021 <b>BCBP Canaveral</b> 321-783-2066 <b>State Warning Point</b> 800-320-0519 <b>ICE Jacksonville</b> 904-232-2611 <b>ICE Canaveral</b> 321-452-3700</p>
	<p>Make thorough initial report of situation, including location and description of cargo/object and whether it is:</p> <p><input type="checkbox"/> A <b>Watch List</b> item not a spill or release;</p> <p><input type="checkbox"/> An actual release including substances emitting radiation (e.g., cracked container with suspicious powdered substance leaking out, with or without radiological alarms); or</p> <p><input type="checkbox"/> A radiological detector or pager alarm related to a sealed package or shipping container.</p>	
	Gather shipping papers and Material Safety Data Sheets if possible to provide additional info once responders arrive.	
	Evacuate all personnel from areas of suspected chemical, biological, or radiological contamination. In the event of a radiological alert related to a sealed package or shipping container, evacuate to a radius appropriate to the level of emissions	
	Discontinue all cargo and bunker operations in the immediate vicinity of the suspect cargo / object. Conduct an “ <b>OPERATIONAL PAUSE</b> ” review of personnel, operations, and possible planted devices in the facility, and all vessels docked to the facility (when detected pier-side).	
	Do not remove the container from vessel or facility unless instructed by law enforcement authorities.	
	Rig fire hoses in case of radiological contamination and stay upwind, uphill, and upstream from suspected release.	
	<p><b>If aboard a vessel underway...</b></p> <p><input type="checkbox"/> Anchor vessel away from other vessels. Do not bring vessel into port – await specific directions regarding movement of the vessel from the Coast Guard Integrated Command Center (ICC) on VHF Channel 16 and/or 22A.</p> <p><input type="checkbox"/> Do not allow any supply vessels, bunker vessels, or pilot boats near vessel.</p> <p><input type="checkbox"/> Do not allow any personnel to board vessel unless directed by authorities.</p>	
	Activate vessel’s or facility’s security plan.	

## Recommended Initial Facility/Vessel Response Structure:



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 5 -1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

**Recommended Reinforced Unified Response Structure:**



VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 5 -2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

## Area Maritime Security Plan SUSPECT ITEM WATCH LIST

Many items, substances, and devices closely resemble controlled items under a variety of U.S. and international treaties and laws directed toward prevention of proliferation and terrorism. In many cases, items are “dual use,” meaning the object may be legally used for certain purposes, but may also be used to for chemical, biological, or nuclear weapons (including “dirty bomb”) purposes. Accordingly, if any item appearing to be one of the items on this Watch List is observed, it should be considered suspect; a much more detailed investigation will likely be required to determine whether the item is in fact controlled/dangerous. Further, even controlled items may be legally shipped with appropriate approvals. This list should trigger further investigation, but should not be interpreted as definitive proof the item is controlled.

### Controlled Nuclear Items, Substance, or Devices

- ☐ N-1: Un-declared or mis-declared item or substances bearing the “N” stamp, or unexplained N-Stamp items in an unusual location (e.g., in crew or engineering spaces aboard a ship, in a general cargo container, or other smuggling-type location)
- ☐ N-2: Un-declared or mis-declared items or substances bearing any indication that they contain Uranium 232, Uranium 235, Plutonium 239, or UF<sub>6</sub> (a radioactive gas)
- ☐ N-3: Any un-declared or mis-declared items or substances that emit radiation above background levels, and any declared item emitting radiation above the level to be expected from the declared material
- ☐ N-4: Any un-declared or mis-declared item with a Hazardous Material label or placard indicating radioactive materials (Class 7), or an unexplained Hazardous Material Class 7 labeled item in an unusual location (e.g., in crew quarters or in a delivery truck).

### Controlled Biological Warfare Items, Substances, or Devices

- ☐ B-1: Un-declared, mis-declared, or unusual (exotic) biological growth media (petrie dishes), particularly media with biological growth in-progress (versus unused media)
- ☐ B-2: Un-declared or mis-declared biological incubators or unexplained incubators in an unusual location (e.g., in crew or engineering spaces aboard a ship, in a general cargo container)
- ☐ B-3: Un-declared or mis-declared bio-safety suits, or unexplained biosafety suits in an unusual location (e.g., mixed with crew fire suits, in personal luggage)
- ☐ B-4: Un-declared or mis-declared biological isolation chambers, or unexplained biological isolation chambers in an unusual location (e.g., aboard a merchant ship or in a delivery truck)
- ☐ B-5: Un-declared or mis-declared biological fermentor machinery (used to grow large numbers of micro-organism), or unexplained incubators in an unusual location (e.g., aboard a merchant ship or in a delivery truck). Fermentors range in size from hand-portable through desktop to free-standing sizes.
- ☐ B-6: Any un-declared or mis-declared item with a bio-hazard label/placard, or an unexplained bio-hazard labeled item in an unusual location (e.g., in crew quarters or in a delivery truck).

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 5 -3
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------

- ☐ **B-7:** Any un-declared or mis-declared Nunc vials, cryogenic vials, or any vials in cryogenic storage (liquid Nitrogen), or unexplained vials/storage in an unusual location.
- ☐ **B-8:** Any un-declared or mis-declared item appearing to be a dispersion device (for spreading/spraying vapors, powders, or liquid mists), or an unexplained dispersion device in an unusual location. There are three general classes of dispersion devices: canisters/packets attached to explosives (including small explosives such as fire-crackers or fireworks), aerodynamic devices (sprayers), and thermal devices (the substance is spread on a heat-producing devices, primarily to spread vapors).
- ☐ **B-9:** Any un-declared or mis-declared item on the Center for Disease Control's Select Agents List or the United Nation's High Consequence Pathogens and Toxins list.
- ☐ **B-10:** Any un-declared or mis-declared item with a Hazardous Material label or placard indicating infectious substance (Class 6, Division 6.2), or an unexplained Hazardous Material Division 6.2 labeled item in an unusual location (e.g., in crew quarters or in a delivery truck).

### Controlled Chemical Warfare Items, Substances, or Devices

- ☐ **C-1:** Un-declared or mis-declared Chemical-safety suits, or unexplained Chem-safety suits in an unusual location (e.g., mixed with crew fire suits, in personal luggage)
- ☐ **C-2:** Any un-declared or mis-declared item with a Hazardous Material label or placard indicating gasses toxic by inhalation (Class 2, Division 2.3), toxic materials (Class 6) or corrosive (Class 8), or an unexplained Hazardous Material labeled item in an unusual location (e.g., in crew quarters or in a delivery truck).
- ☐ **C-3:** Any un-declared or mis-declared exotic canister or container (glass-lined, exotic stainless-steel alloys, etc.), or any unexplained exotic canisters in an unusual location.
- ☐ **C-4:** Any un-declared or mis-declared item appearing to be a dispersion device (for spreading/spraying vapors, powders, or liquid mists), or an unexplained dispersion device in an unusual location. There are three general classes of dispersion devices: canisters/packets attached to explosives (including small explosives such as fire-crackers or fireworks), aerodynamic devices (sprayers), and thermal devices (the substance is spread on a heat-producing devices, primarily to spread vapors).
- ☐ **C-5:** Any un-declared or mis-declared item on the Chemical Warfare Convention's Schedule One list of Chemical Warfare agents (CW agents fall into the following classes: Blister Agents, Blood Agents, Asphyxiating Agents, Incapacitating Agents, and Nerve Agents)

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	Tab C 9600 TSI 5 -4
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------------------------



Immediate Response Actions:		
✓	Response Action	Notes
	Make thorough initial report of situation including as many details as possible about crewman. <b>Notify authorities immediately.</b> Take crewman into custody.	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b> <b>ICE Jacksonville</b> <b>904-232-2611</b> <b>ICE Canaveral</b> <b>321-452-3700</b> <b>FBI</b> <b>904-721-1211</b>
	Maintain communications with authorities and report changes in situation.	
	Call facility or vessel security to verify that a particular activity is to occur. Update authorities if the activity turns out to be legitimate.	
	Conduct search of facility or vessel for Trespassing Persons, Explosive Devices, signs of Tampering, and CBRNE devices.	
	<b>Examples of Suspicious Activity:</b> <ul style="list-style-type: none"> <li>Unknown or unauthorized person (s)</li> <li>Taking photographs of vessels, facility or infrastructure</li> <li>Loitering in vicinity of facility, vessel, or unauthorized area</li> <li>Calling facility to learn security procedures</li> <li>Soliciting information about vessel, facility from employees</li> <li>Attempting to stow or drop-off suspicious packages</li> <li>Attempting to access unauthorized areas, FSP or VSP.</li> <li>Discovery of unauthorized weapons.</li> <li>Discovery of subversive material.</li> </ul>	
	Activate vessel or facility security plan.	

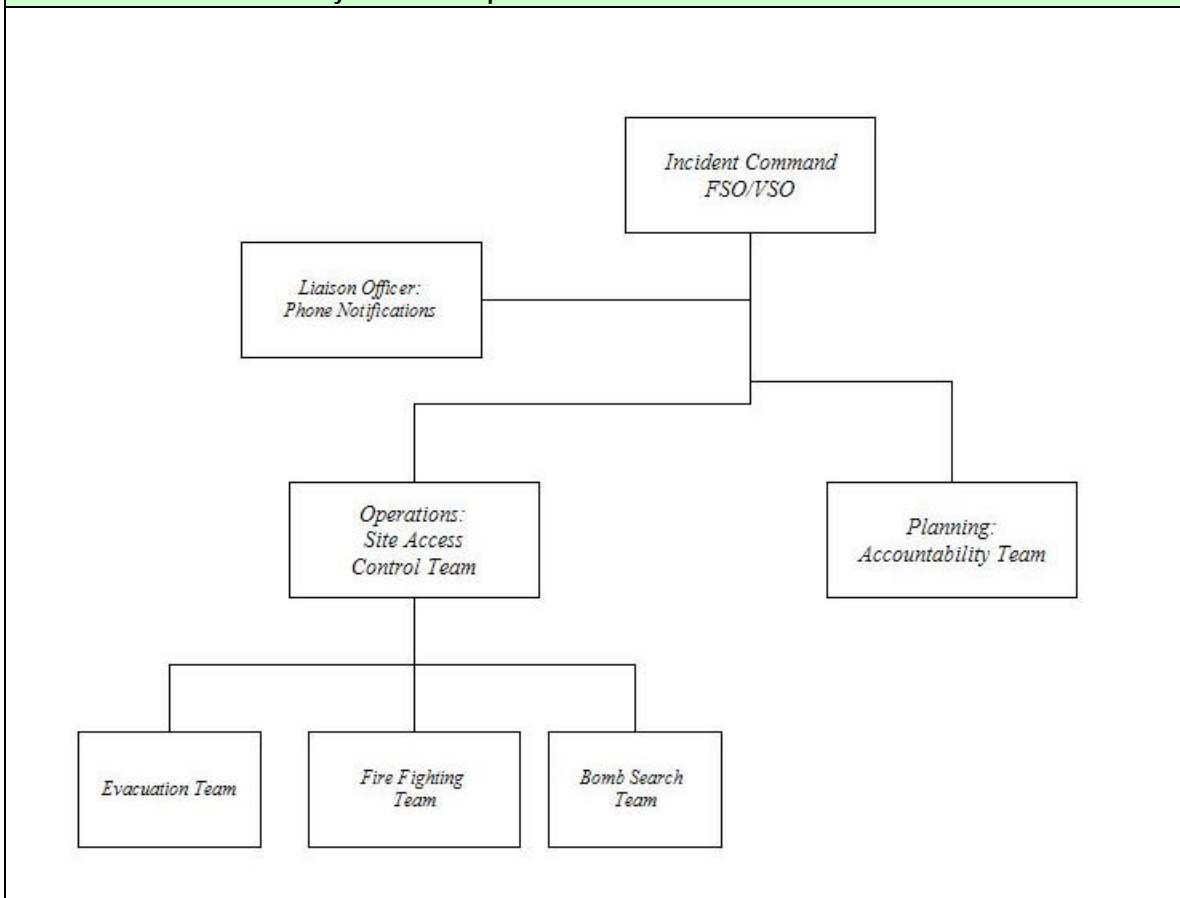
Recommended Initial Facility/Vessel Response Structure:	
<p><b><u>OVERT ACTION</u></b></p> <pre> graph TD     IC["Incident Command: FSO/VSO"] --- L["Liaison: Phone Notifications"]     IC --- OT1["Operations: Search Team"]     IC --- OT2["Operations: Detainment Team"] </pre>	<p><b><u>PASSIVE CONCERNS</u></b></p> <p><b>FSO/VSO will monitor individual and stay in contact with local authorities.</b></p> <p><b>Report suspicious activities as directed.</b></p>

# EXPLOSION IN PORT

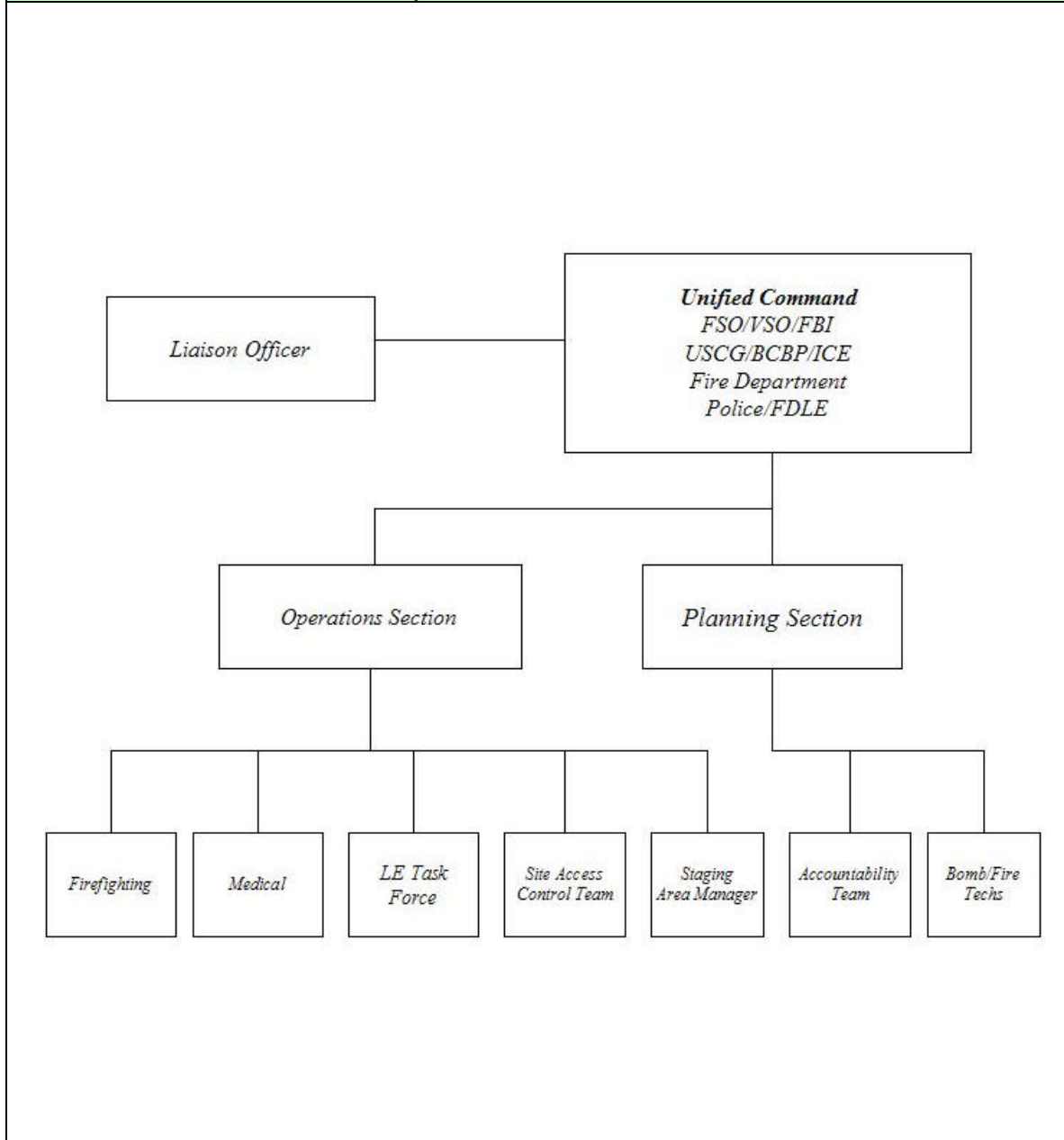
## Immediate Response Actions:

✓	Response Action	Notes
	Activate vessel or facility security plan. Make notification to authorities.	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b> <b>ICE Jacksonville</b> <b>904-232-2611</b> <b>ICE Canaveral</b> <b>321-452-3700</b>
	Secure vessel or facility against potential intrusion.	
	Evacuate to a predetermined location if evacuation is determined to be necessary. Prescreen location for safety and possible <b>secondary device</b> prior to mass arrival.	
	If not directed to evacuate, cease all transits and transfers until situation is resolved.	
	If transiting, expect USCG UMIB on VHF Channel 16. Follow direction and anticipate waterway to be closed.	

## Recommended Initial Facility/Vessel Response Structure:

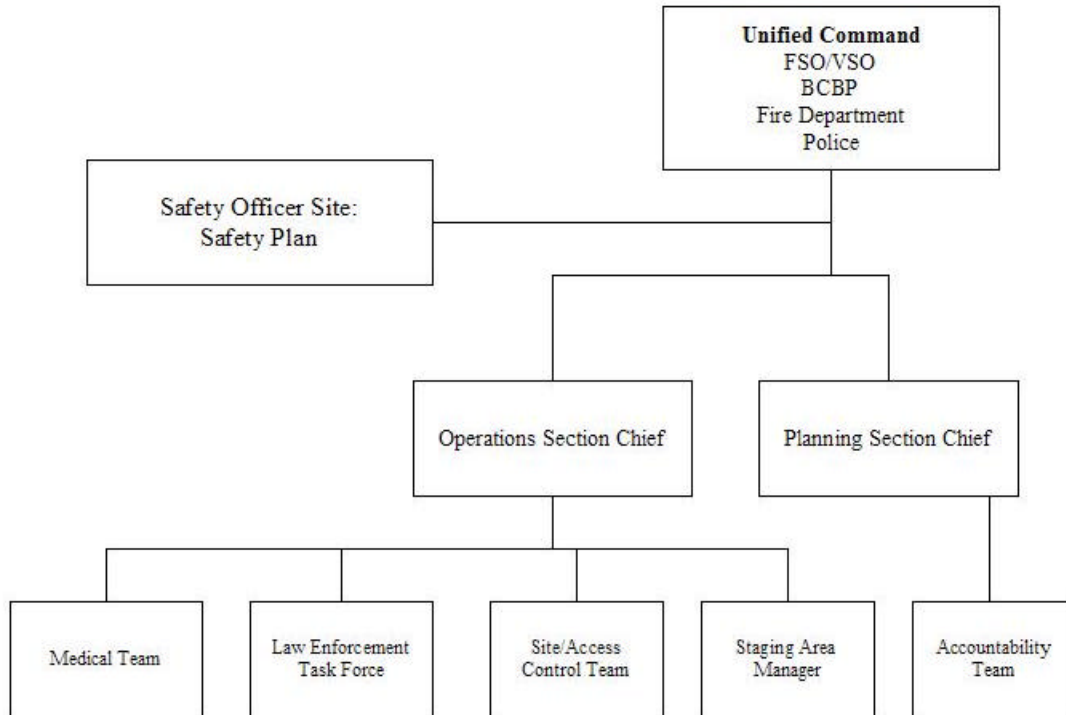


## Recommended Reinforced Unified Response Structure:



Immediate Response Actions:		
✓	Response Action	Notes
	Make thorough initial report of observed activity and on scene conditions. Include vessel description, any visible registration numbers, and descriptions of and numbers of personnel on board.	<b>Police &amp; Fire 911</b> <b>USCG 904-247-7318</b> <b>NRC 800-424-8802</b> <b>BCBP Jacksonville</b> <b>904-360-5021</b> <b>BCBP Canaveral</b> <b>321-783-2066</b> <b>State Warning Point</b> <b>800-320-0519</b>
	Inform the master of the vessel that he/she is in a security zone and will need to clear the area.	
	Monitor actions of the vessel (s) and report all behavior of personnel onboard.	
	If vessel places any object (s) into water, provide details and location of object(s)	
	Activate nearby vessel and facility security plans.	
	Secure vessels and facilities against forced entry.	
	Set up Incident Command Post.	
	Contact delivery companies, oncoming workers and adjacent facilities to prevent conflict outside the facility or vessel.	
Recommended Initial Facility/Vessel Response Structure:		
<pre> graph TD     IC["Incident Command: FSO/NSO"]     L["Liaison: Phone Notifications"]     O["Operations: Site/Access Control Team"]     P["Planning Accountability Team"]      IC --- L     IC --- O     IC --- P         </pre>		

## Recommended Reinforced Unified Response Structure:



# PORT-WIDE MASS EVACUATION

## Response Action for Facility, Company or Moored Vessel

✓	Response Action	Notifications
	Facility/Company/Vessel receives and acknowledges receipt of Mass Evacuation order from FMSC or other recognized authority.	USCG 904-247-7318 VHF Channel 16/22A
	Notify/Communicate the Mass Evacuation order to Facility/Company/Vessel security officer, as appropriate.	
	Activate facility/company/vessel security plans and notify adjacent facilities/vessels.	
	Determine the need for immediate personal protective measures.	
	Select and communicate the incident command post location.	
	Establish incident command (ICS or Unified) structure.	
	Develop Incident Objectives and Incident Action Plan.	
	Secure all facility/vessel operations.	
	Perform traffic control, crowd control functions at facility.	
	Pass the notification to all tenants and vessels docked in the port.	
	Ensure full personnel accountability during mass evacuation.	
	Report “Evacuation Complete” to FMSC or other recognized authority as appropriate.	

## Response Action for Vessel Underway within Port Limits

✓	Response Action	Notifications
	Vessel receives Mass Evacuation order from FMSC or other recognized authority.	USCG 904-247-7318 VHF Channel 16/22A
	Notify/Communicate the Mass Evacuation order to Company/Vessel security officer, as appropriate.	
	Activate vessel security plans and notify nearby unaware vessels.	
	Determine the need for immediate personal protective measures.	
	Await specific instructions regarding vessel movement via Urgent Marine Information Broadcast from the US Coast Guard Integrated Command Center (ICC) on VHF Channel 16 and/or 22A.	

## Recommended Facility/Vessel Response Structure:



---

# **Charter**

## **of the**

### **JMTX Port Security Committee**

## **and**

### **Port Canaveral Security Committee**

This document charters the Jacksonville Maritime Transportation Exchange (JMTX) Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee, in accordance with Title 33 Code of Federal Regulations Section 103.300(b). Together, these port security committees fulfill the requirements of that regulation regarding Area Maritime Security Committees. This charter is organized as follows:

- Organization
- Rules Governing the Port Security Committees
- Rules Governing the Working Subcommittees
- Rules Governing the Executive Subcommittee
- Handling and Protection of Information
- Amending the Charter

## **Organization**

This section outlines the organization of the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal Regulations Section 103.305(a). This section is organized as follows:

- JMTX Jacksonville/Fernandina Port Security Committee
- Port Canaveral Security Committee
- Standing Committees
- Ad-Hoc Committees

## **The JMTX Jacksonville/Fernandina Port Security Committee**

The Jacksonville Marine Transportation Exchange (JMTX) is Jacksonville's maritime trade organization created to work for the success of its membership and coordinate the safe, secure and environmentally responsible management of the marine transportation system within the port of Jacksonville. JMTX's goal is to work in partnership with the port stakeholders to make Jacksonville the port of choice.

Somewhat unique as a maritime association, JMTX has been established to provide a stable coordinating structure for port-wide planning, coordination and infrastructure recommendations. JMTX serves as an information clearinghouse for port critical information, provides a forum for stakeholder issues and serves as a stakeholder advocate to local, regional and national agencies.

JMTX is a growing organization with more than 55 member companies and agencies. JMTX is structured around seven critical committees including: Port Security, Harbor Safety, Information Sharing, Maritime Infrastructure, Agents and Operators, Community Outreach and Environmental Protection. Port stakeholder involvement in these committees is wide spread and has not been limited to JMTX members.



---

JMTX has been accepted by the U. S. Coast Guard as the coordinating organization for the port's official Port Security Committee, and the Harbor Safety Committee. Since 9/11, JMTX has played a major role in coordinating security issues including assessments, intelligence sharing and compliance with security requirements.

The JMTX Jacksonville/Fernandina Port Security Committee brings together the resources and experience of law enforcement, regulatory agencies and port stakeholders to develop strategies and procedures to support the goals of port security.

The committee is jointly chaired by the Coast Guard Captain of the Port along with an industry leader.

## **The Port Canaveral Security Committee**

The Port Canaveral Security Committee is a standing body of industry leaders, Department of Defense representatives, Port Authority representatives, NASA representatives, port law enforcement agencies, and emergency response contractors and governmental agencies. For many years, this informal body has worked with the Coast Guard Captain of the Port in Jacksonville and the Marine Safety Detachment in Port Canaveral to coordinate the safe, secure and environmentally responsible management of the marine transportation system in Port Canaveral and the surrounding area.

The Port Canaveral Security Committee has been accepted by the U. S. Coast Guard as the port's official Port Security Committee. Since 9/11, the Port Security Committee has played a major role in coordinating security issues including assessments, intelligence sharing and compliance with security requirements.

The Port Canaveral Security Committee brings together the resources and experience of law enforcement, regulatory agencies and port stakeholders to develop strategies and procedures to support the goals of port security.

The committee is jointly chaired by the Coast Guard Captain of the Port's representative along with an industry leader.

## **Standing Subcommittees**

The JMTX Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee standing subcommittees shall generally be established/disestablished on the direction of the Co-Chairs to address long term issues or goals of either PSC. Any PSC Member may volunteer to serve on any standing subcommittee (except the Executive Subcommittee, see section 2345 below). An appointed member of the Executive Subcommittee shall chair each subcommittee. Co-Chairs of the PSC cannot service as Subcommittee Chairpersons. Chairpersons are responsible for the general supervision and coordination of the subcommittee, including scheduling meetings and recording results. Standing Subcommittees include:

- The Executive Subcommittee
- Subcommittee One: Regulatory Compliance and Membership
- Subcommittee Two: Port Security Planning
- Subcommittee Three: Security Exercise Planning and Evaluation
- Subcommittee Four: Special Events Planning
- The Maritime Joint Task Force

## **Ad-Hoc Subcommittees**

The JMTX Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee Ad-Hoc Subcommittees shall be chartered by the Co-Chairs to address specific issues or functions that are expected to be short term. Ad Hoc Subcommittees shall not normally remain active for more than one year.

---

## Rules Governing the Port Security Committees

This section outlines the rules governing the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal Regulations Section 103. This section is organized as follows:

- Purpose and Scope of the Committees
- Membership in the Committees
- Meetings of the Committees
- Geographic Area of Responsibility of the Committees

### Purpose and Scope of the Committees

**JMTX Jacksonville/Fernandina Port Security Committee.** The JMTX Jacksonville/Fernandina Port Security Committee exists to accomplish the following three goals:

- 1) The Port Security Committee will assist agencies and organizations with meeting the statutory requirements from both state and federal Seaport Security measures.
- 2) The Port Security Committee will support and assist the Federal Maritime Security Coordinator (USCG Captain of the Port), state and local agencies, and maritime stakeholders with assessment, planning and exercising of port security issues.
- 3) The Port Security Committee will serve as a forum for the exchange of intelligence, experience and ideas relating to maritime security issues.

**Port Canaveral Security Committee.** The Port Canaveral Security Committee provides a forum for port stakeholders in and near Port Canaveral to evaluate maritime vulnerabilities to terrorism and criminal activities and works to assist in the formulation of protection strategies and plans. The Committee also provides a link between law enforcement agencies and port industry members to help coordinate planning and activities.

### Membership in the Committees

**JMTX Jacksonville/Fernandina Port Security Committee.** All persons, firms, associations, agencies, and corporations of good standing in the community are eligible for membership in the Jacksonville Maritime Transportation Exchange and are free to join the Port Security Committee.

**Port Canaveral Security Committee.** All persons, firms, associations and corporations of good standing in the community are eligible for membership in the Port Security Committee. Membership is open to any interested commercial entity, government agency, or other marine transportation system stakeholder operating on, or along, or having jurisdiction over Port Canaveral and surrounding navigable waterways.

---

## Meetings of the Committees

Each Port Security committee shall meet as needed and called by the chair, and in any case not less than once during each calendar year and preferably once each quarter. Additionally, the committee will meet when requested by a majority of the AMS committee members. The Chair shall determine the time and venue of the meetings. The Chair shall make arrangements for these meetings, preferably with a revolving “host” from amongst the subcommittee members. Meetings shall be open to the public and shall not cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information. Records of these meetings may be made available to the public upon request. However, FMSC’s will ensure that all material designated as SSI will be protected from disclosure to the public.

## Geographic Area of Responsibility of the Committees

The area covered by this plan is defined in federal regulations at Title 33 Code of Federal Regulations part 3.35-20. In general, the area of Northeast Florida (including the extreme southern border area of Georgia) and Eastern Central Florida for which Port Security Committees have been established are divided as follows:

- **JMTX Port Security Committee** – Northeast Florida including those parts of Baker, Clay, Duval, Flagler, Nassau, Putnam, and St. Johns Counties in Florida and Camden and Charlton Counties in Georgia, which fall within the bounds described in 33 CFR part 3.35-20.
- **Port Canaveral Security Committee** – Eastern Central Florida including those parts of Brevard, Lake, Volusia, Seminole, Orange, and Osceola Counties, Florida, which fall within the bounds described in 33 CFR part 3.35-20.

## Rules Governing the Working Subcommittees

This section outlines the rules governing working subcommittees of the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal Regulations Section 103. This section is organized as follows:

- Purpose and Scope of the Subcommittees
- Membership in the Subcommittees
- Officers of the Subcommittee
- Meetings of the Subcommittees Procedural Rules

## Purpose and Scope of the Working Subcommittees

The purpose of the Port Security Committee’s Working Subcommittees is to form a small, balanced nucleus of port stakeholders that meet the goals and objectives of the Port Security Committee. Specific objectives of the working subcommittees are:

### **Subcommittee One: Regulatory Compliance and Membership**

- Provide a regular forum for discussion of information relative to state and federal legislation and rulemaking.
- Provide a unified response to state and federal legislators to effect common rules for implementation.
- Assist stakeholders in the implementation of federal and state regulations.
- Sponsor Maritime Domain Awareness infrastructure for the port.

### **Subcommittee Two: Port Security Planning**

- 
- **Area Maritime Security Plan:** Develop and execute a whole-port security coordination plan (similar to the Area Contingency Plan for pollution response) for all commercial and private stakeholders, and federal, state, and local government agencies with responsibilities in the port or on the waterways of Jacksonville.
  - **“One-Method” Consensus Risk Assessment Methodology:** Develop and deploy a consensus Risk (consequence \* vulnerability\*threat) assessment methodology to be used by all government and private entities in the port.
  - **“One-Format” Consensus Vessel and Facility Security Plan Templates:** Develop and deploy consensus vessel and facility security plan templates/formats which are based on the “one-method” risk assessments and which incorporate all government agency requirements.
  - **Develop Expertise:** Provide a support system in form of training, review, and comment to private companies and government agencies as they begin using the “one-method” Risk Assessment Methodology and “one-format” vessel and facility security plan templates.

#### **Subcommittee Three: Security Exercise Planning and Evaluation**

- **Annual Port Security Drills.** Design and execute Area Maritime Security Drills in the port at least once per year to exercise and improve the Area Maritime Security Plan for the port.
- **Stakeholder Drills.** Assist port stakeholders with the design and execution of their security drills and exercises as required by federal, state, and local regulation.
- **Collect and Share Best Practices.** Capture and share the lessons learned during exercises and develop best practices to share with all port stakeholders.

#### **Subcommittee Four: Special Events Planning**

- Synthesize special event security plans in coordination with the Maritime Joint Task Force and Subcommittee Two.

#### **Maritime Joint Task Force (Government)**

- Provide an intelligence briefing at the quarterly PSC General Membership meeting. The briefings will be in accordance with applicable state and federal laws related to classified information.
- Provide a two-way communication mechanism to provide critical port security information among law enforcement agencies and port stakeholders.
- Assist security incident prevention and response agencies to coordinate and cooperate.
- Through a series of Memoranda of Agreement between federal, state, and local government agencies, establish a systematic, standing joint agency security activity/patrol/mission planning and de-conflicting (JMP/D) process. The systematic process must assure the agencies: (1) jointly plan and conduct overlapping operations; (2) fully leverage each other's independent operations for mutual benefit; and (3) avoid unintentionally infringing upon each other's operations or unintentionally imposing redundant burdens on our customers.

## **Membership in the Subcommittees**

Members will be assigned to serve in Subcommittees on a volunteer basis. Any general member of the Port Security Committee is eligible for membership in any subcommittee, except the Maritime Joint Task Force, which is composed solely of government agency representatives. Members will not be appointed and membership in the subcommittee will be highly informal and based on the member's willingness to serve.

Subcommittee members will not be required to submit to a security background examination.

## **Officers of the Subcommittees**

The Chair of the each Subcommittee for each Port Security Committee will be a designated member of the Executive Subcommittee only. No other subcommittee officers need be appointed in order to maintain the open and informal working environment.

---

## Meetings of the Subcommittees

Each Executive Subcommittee shall meet as needed and called by the chair, and any case not less than once during each calendar year and preferably once each quarter. The Chair shall determine the time and venue of the meetings. The Chair shall make arrangements for these meetings, preferably with a revolving “host” from amongst the subcommittee members. Meetings shall be open to the Port Security Committee and shall not cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information. The Executive Subcommittee Chair shall schedule meetings to cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information restricted to the appointed members and select expert invitees separately; rules governing those sessions are described in section 2340 below.

## Working Subcommittee Procedural Rules

**Rule 1. Subcommittee Policy.** It is the policy of the Subcommittees that Port Security Committee members shall have the opportunity to speak to any Subcommittee meeting agenda item before final action.

**Rule 2. Scheduling of Closed Session.** Bearing in mind section 2351 of this charter (below), special closed sessions shall be scheduled to the extent possible and appropriate prior to Port Security Committee membership meetings. Any closed session may be scheduled during or after a general Port Security Committee meeting.

**Rule 3. Meeting Adjourned to Date Certain.** When a Subcommittee meeting is adjourned, it must in all cases be adjourned to another scheduled meeting date. All unfinished items will be listed in their original order after roll call on the agenda of such scheduled meeting.

**Rule 4. Agenda Matters.** The principle procedure for holding Subcommittee meetings will be an agenda. All meetings shall have an agenda.

**Rule 5. Quorum.** Subcommittees shall have no quorum and shall meet with any number of members present.

**Rule 6. Minutes.** The Subcommittees shall not be required to prepare and distribute minutes of its meetings. The Chair shall take notes; these notes need not be verbatim but shall reflect the sense of the discussion and any recommendation made with respect to each subject considered in subcommittee. A report of the subcommittee shall be delivered to the Port Security Committee during its quarterly meetings and to the Federal Maritime Security Coordinator upon request.

**Rule 7. Conduct of Subcommittee Meetings.** The chair of the Subcommittee may conduct meetings with as much informality as is consistent with these charter procedural rules. The views of interested private citizens may be heard in certain subcommittee meetings, but in no case shall a subcommittee meeting be used as a substitute for the Port Security Committee meetings.

## Rules Governing the Executive Subcommittee

This section outlines the rules governing the executive subcommittee of the JMTX Jacksonville/Fernandina Port Security Committee (PSC) and the Port Canaveral Security Committee (PCSC) in accordance with Title 33 Code of Federal Regulations Section 103. This section is organized as follows:

- Purpose and Scope of the Executive Subcommittee
- Membership in the Executive Subcommittee
- Nomination and Appointment Process
- Acceptance and Pledge
- Officers of the Subcommittee
- Meetings of the Subcommittee

- 
- Procedural Rules

## **Purpose and Scope of the Executive Subcommittee**

The purpose of the Port Security Committee's Executive Subcommittee is to form a small, balanced nucleus of port stakeholders that steer the work of the Port Security Committee and meet the requirements for an Area Maritime Security Committee (AMSC), consistent with Title 33 Code of Federal Regulations Section 103.310. Responsibilities of the Executive Steering Subcommittee are:

- To chair the working subcommittees;
- To identify critical port infrastructure and operations;
- To identify risks (threats, vulnerabilities, and consequences) in the maritime sector;
- To complete an Area Maritime Security Assessment in accordance with 33 CFR Part 103, subpart D;
- To determine mitigation strategies appropriate to these risks and implementation methods;
- To develop and describe the process for continually evaluation the overall port security by considering consequences and vulnerabilities, how they change over time, and what additional mitigation strategies can be applied;
- To provide advice to and assist the Federal Maritime Security Coordinator in developing the Area Maritime Security Plan in accordance with 33 CFR Part 103 Subpart E;
- To design and recommend to the Federal Maritime Security Coordinator measures to assure effective security of infrastructure, special events, vessels, passengers, cargo and cargo handling equipment at facilities within the port and not otherwise covered under federally approved Vessel or Facility Security Plans;
- To serve as the principle link for communicating the Area Maritime Security Plan once approved, including any requirements for entities operating in the port contained in the Plan;
- To serve as the principle link for communicating threats and changes in Maritime Security Condition (MARSEC) levels;
- To serve as the principle link for disseminating appropriate security information to the Port Stakeholders;
- To serve to assist entities operating in the port in understanding and complying with Federal, State, and Local security regulations and requirements;
- To coordinate governmental security incident command-and-response through one of the AMSC subcommittees;
- To audit and revise the Area Maritime Security Plan on a regular basis and following experiences offering lessons learned;
- To coordinate the conduct of an Area Maritime Security Exercise at least once each calendar year;
- To maintain records of Port Security Committee operations and decisions.

## **Membership in the Executive Subcommittee**

In accordance with Title 33 Code of Federal Regulations Section 103.305 (Composition of an Area Maritime Security Committee), the Executive Subcommittee must have not less than seven and no more than 50 (total) members appointed by the Federal Maritime Security Coordinator, each having at least five years experience related to maritime or port security operations (including broad state or local counter-terrorism responsibilities). The Executive Subcommittee members serve as the core or steering group for the JMTX Jacksonville/Fernandina Port Security Committee and the Port Canaveral Security Committee. Members will be assigned to serve on the JMTX Jacksonville/Fernandina Port Security Committee or the Port Canaveral Security Committee, but not both, in their Appointment Letter from the Federal Maritime Security Coordinator. Appointments will typically be for a five year period; members may be reappointed where warranted and furthering the purposes of the Executive Subcommittee.

Prior to appointment, nominated members will be required to submit to appropriate security background examinations to verify the identity and suitability of the nominee.

---

To be considered for appointment, nominees must be members in good standing of one of the following:

- Federal Governmental Agencies with Authority, Jurisdiction, or Interest in Maritime Homeland Security in Northeast Florida;
- State Governmental Agencies or Political Officials with Authority, Jurisdiction, or Interest in Maritime Homeland Security in Northeast Florida;
- Local public safety, crisis management, and emergency response agencies in Northeast Florida;
- Law enforcement agencies in Northeast Florida;
- Security organizations in Northeast Florida;
- Maritime industry;
- Other port entities or individuals having special competence in maritime security; or
- Other port entities or individuals likely to be affected by security practices and policies.

## **Nomination and Appointment Process**

The Federal Maritime Security Coordinator will, at his sole discretion, solicit the Port Security Committees for nominations for appointment to the Executive Subcommittee. Nominations will typically be made in writing to the Port Security Committee Co-Chairs. Nominations must detail how the nominee meets the requirements of section 2342 of this charter, and must explicitly state the willingness of the individual both to serve and to submit to the required security background examinations. Nominations may be submitted by the nominee him or herself, or by other persons. When a nomination is for another person, it must explicitly state whether the individual is aware of the nomination and is willing to serve.

Once the announced period for submitting nominations to the Executive Subcommittee elapses, the Port Security Committee Co-Chairs will compile lists and background information on all nominees and consult with the Executive Subcommittee on these nominees. Based on a majority vote, the Executive Subcommittee will forward a list of nominees recommended for appointment to the Federal Maritime Security Coordinator for final evaluation. When the nominations are deemed insufficient for the purposes of the Executive Subcommittee, the Subcommittee may take action to recruit nominations from individuals who had not considered appointment, and may reconvene to consider these additional nominations. In no case shall this process extend more than 30 days after the close of the announced period.

In consultation with the Port Security Committee Co-Chairs, the Federal Maritime Security Committee will review the Executive Subcommittee's recommendations for appointment and make such appointments as are consistent with 33 CFR 103.305, this charter, and the purpose of the Subcommittee. The Federal Maritime Security Coordinator will then conduct the required security background checks and extend letters of appointment to selected members.

Appointed members must indicate their intention to accept or decline the appointment and abide by the appointment as outlined in section 2344 of this charter, below. Members not accepting this appointment will return to general Port Security Committee membership status.

The Federal Maritime Security Coordinator will revoke any appointment at any time whenever he or she concludes such action is necessary for the efficient or effective functioning of the Executive Subcommittee, or when he or she concludes that the appointed member is not participating sufficiently to accomplish purposes of the Port Security Committees or the work of the Executive Subcommittee.

## **Acceptance and Pledge**

Once nominated, qualified candidates accepted by the Federal Maritime Security Coordinator will be accepted as appointed members of the Executive Subcommittee by pledging to abide by the rules of this charter and to act in good faith and to the best of their ability in the application of the policies and procedures established by the Executive Subcommittee. Executive Subcommittee members shall indicate their adoption of this pledge by affixing to their appointment letter or a copy thereof the signature of both the member and his or her supervisor (where appropriate). The Subcommittee Member shall return a signed copy of the appointment letter to the Port Security Committee Co-Chairs. Subsequent intent by a member



---

to withdraw from the Executive Subcommittee shall be conveyed to Co-Chairs through written notification. Appointed members are not authorized to deputize assistance or others to attend Port Security Meetings or Executive Subcommittee Meetings on their behalf; continuity of participation and fluency in the issues at hand will not permit this practice.

The Port Security Committee Co-Chairs shall periodically request the Executive Subcommittee review, and if necessary revise, the total numbers and composition of the Subcommittee. When changes are approved, the Co-Chairs will request nominations and make appointments as outlined in Section 2343 above.

## Officers of the Executive Subcommittee

The Chair of the each Executive Subcommittee for each Port Security Committee shall be elected by that Executive Subcommittee only, not by the body of the whole Port Security Committee, and shall be an appointed member of that Executive Subcommittee. The Chair shall appoint, with the consent of the Executive Subcommittee, a Secretary and a Chair for each of that PSC's Working Subcommittees from among the appointed members. The policies and procedures of the Port Security Committee, either by consensus or vote, shall be recorded and publicized by the Secretary. The Secretary shall also record and publish minutes of each Port Security Committee meeting and maintain a list of active PSC members. The Secretary shall also maintain a list of the Executive Subcommittee members. Officers shall retain voting privileges during their terms of service.

## Schedule of Meetings

Each Executive Subcommittee shall meet at least once during each calendar year and preferably once each quarter. The time and venue of the meetings shall be determined by the Executive Subcommittee Chair and members. Arrangements for these meetings shall be made by the Executive Subcommittee Chair. Annual and Quarterly meetings shall be open to the Port Security Committee and shall not cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information. The Executive Subcommittee Chair shall schedule meetings to cover Security Sensitive, Classified, Proprietary, or Commercially Sensitive Information restricted to the appointed members and select expert invitees separately; rules governing those sessions are described in section 2351 below.

## Executive Subcommittee Procedural Rules

**Rule 1. Executive Subcommittee Policy.** It is the policy of the Executive Subcommittee that Port Security Committee members shall have the opportunity to speak to any Executive Subcommittee meeting agenda item before final action.

**Rule 2. Spokesperson for a Group of Persons.** When any group of persons wishes to address the Executive Subcommittee on the same subject matter, it shall be proper for the presiding officer to request that a spokesperson be chosen by the group to address the Subcommittee.

**Rule 3. Scheduling of Closed Session.** Bearing in mind section 2351 of this charter (below), special closed sessions shall be scheduled to the extent possible and appropriate prior to Port Security Committee membership meetings. Any closed session may be scheduled during or after a general Port Security Committee meeting.

**Rule 4. Meeting Adjourned to Date Certain.** When an Executive Subcommittee meeting is adjourned, it must in all cases be adjourned to another scheduled meeting date. All unfinished items will be listed in their original order after roll call on the agenda of such scheduled meeting.

**Rule 6. Agenda Matters.** The principle procedure for holding Executive Subcommittee meetings will be an agenda. All meetings shall have an agenda.

---

**Rule 7. Presiding officer to state issue.** The presiding officer shall assure that all issues are clearly stated before allowing discussion to begin. The presiding officer may also restate the issue before allowing discussion to continue or prior to voting.

**Rule 8. Presiding officer may discuss and vote.** The presiding officer may move, second and discuss from the chair, subject only to such limitations of debate as are by these rules imposed on all Executive Subcommittee members. The presiding officer shall not be deprived of any of the rights and privileges of a Subcommittee member.

**Rule 9. Quorum.** A majority of the committee membership shall constitute a quorum.

**Rule 10. Referrals.** Referrals to the working subcommittees shall be made by the Executive Subcommittee. Items may be withdrawn from the working subcommittee and taken up for consideration by the Executive Subcommittee at any meeting with the consent of a majority of the Executive Subcommittee members.

**Rule 11. Minutes.** The Executive Subcommittee shall not be required to prepare and distribute minutes of its meetings. Notes shall be taken by the Chair; these notes need not be verbatim but shall reflect the sense of the discussion and any recommendation made with respect to each subject considered in subcommittee. Votes shall be formally recorded including the item voted upon and the total votes for and against. A report of the subcommittee shall be delivered to the Port Security Committee during its quarterly meetings and to the Federal Maritime Security Coordinator upon request.

**Rule 12. Conduct of Executive Subcommittee Meetings.** The chair of the Executive Subcommittee may conduct meetings with as much informality as is consistent with these charter procedural rules. The views of interested private citizens may be heard in certain subcommittee meetings, but in no case shall a subcommittee meeting be used as a substitute for the Port Security Committee meetings.

**Rule 13. Authorization to Vote.** Each appointed member of the Executive Subcommittee may have one vote; votes will not be apportioned according to agency, jurisdiction, or other criterion. With the prior approval of the Federal Maritime Security Coordinator and only in limited exceptional circumstances, a designated alternate may vote in place of an appointed member.

**Rule 14. Manner of Voting.** On the passage of every motion or recommendation to the Federal Maritime Security Coordinator, the vote shall be taken and a formal record of both the motion and votes for and against recorded.

**Rule 15. Silence constitutes affirmative vote.** Executive Subcommittee members who are silent during a voice vote shall have their vote recorded as an affirmative vote, except when individual appointed members have stated in advance that they will not be voting.

**Rule 16. Failure to vote.** It is the responsibility of every appointed Executive Subcommittee member to vote unless disqualified for cause. No appointed AMSC member can be compelled to vote.

**Rule 17. Abstaining from vote.** The abstainer chooses not to vote and, in effect, "consents" that a majority of the quorum of the executive subcommittee members present may act for him or her.

**Rule 18. Not participating.** An Executive Subcommittee member who disqualifies him or herself because of any financial or other interest in the issue at hand shall disclose the nature of the conflict and may not participate in the discussion or the vote. A member may otherwise disqualify him or herself due to personal bias or the appearance of impropriety.

---

**Rule 19. Tie votes.** Tie votes may be reconsidered on motion by any member of the Executive Subcommittee voting aye or nay during the original vote. Before a motion is made on the next item on the agenda, any member of the Executive Subcommittee may make a motion to continue the matter to another date. Nothing herein shall be construed to prevent any member from agendaizing a matter which resulted in a tie vote for a subsequent meeting.

## Handling and Protecting Information

Pursuant to Title 49 Code of Federal Regulations Part 1520, this part governs the release, by the Port Security Committee membership, and by other persons, of records and information that has been obtained or developed during security activities.

For purposes of this section, **Record** includes any writing, drawing, map, tape, film, photograph, or other means by which information is preserved, irrespective of format. **Vulnerability assessment** means any examination of a transportation system, vehicle, or facility to determine its vulnerability to unlawful interference.

Port Security Committee members must restrict disclosure of and access to sensitive security information described in this section to persons with a need to know and must refer requests by other persons for such information to Coast Guard Federal Maritime Security Coordinator.

**Need to know.** For some specific sensitive security information, the Federal Maritime Security Coordinator may make a finding that only specific persons or classes of persons have a need to know. Otherwise, a person has a need to know sensitive security information in each of the following circumstances:

- (1) When the person needs the information to carry out approved, accepted, or directed security duties.
- (2) When the person is in training to carry out approved, accepted, or directed security duties.
- (3) When the information is necessary for the person to supervise or otherwise manage the individuals carrying out approved, accepted, or directed security duties.
- (4) When the person needs the information to advise persons regarding any DHS/DOT security-related requirements.
- (5) When the person needs the information to represent the persons listed in paragraph (1) of this section in connection with any judicial or administrative proceeding regarding those requirements.

**Release of sensitive security information.** When sensitive security information is released to unauthorized persons, any Port Security Committee member or individual with knowledge of the release, must inform the Coast Guard Federal maritime Security Coordinator.

**Violation.** Violation of these rules is grounds for a civil penalty and other enforcement or corrective action.

**These rules will be followed to protect all Security Sensitive Information, Commercial Sensitive Information, and Proprietary Information. Classified Material will be protected in accordance with the rules governing it.**

## Rules for SSI Sessions & SSI Information

---

**Rule 1. Authorized Closed Sessions.** Subject to the advice of the Federal Maritime Security Coordinator and the requirements of 49 CFR Part 1520, closed sessions may generally be held to discuss the following subjects:

- (1) Security matters, i.e., matters posing a threat to the public's right of access to public services or public facilities, as outlined in 49 CFR Section 1520.7, including Security Sensitive Information portions of the Area Maritime Security Assessment and AMS Plan.
- (2) Pending litigation and administrative proceedings prosecuted by or against the Federal Maritime Security Coordinator or Port Security Committees, including but not limited to settlement proceedings.
- (3) Other closed sessions authorized by the Federal Maritime Security Coordinator.

**Rule 2. Calling Closed Sessions.** Subject to the advice of the Federal Maritime Security coordinator, a closed session may be called by the Port Security Committee Co-Chairs or by the Executive Subcommittee.

Closed sessions shall be noticed on the agenda. To the greatest extent possible, the Federal Maritime Security Coordinator and PSC Co-chairs shall use standardized agenda descriptions that are consistent with 49 CFR part 1520.7.

The Port Security Committee shall convene in open session and provide an opportunity for general membership comment as to the closed session items before any closed session. The Co-chairs shall be present in the open session to record any statements made. The Co-Chairs shall announce the item or items to be considered in closed session by reference to the appropriate agenda item, or in an alternate form provided by the Federal Maritime Security Coordinator.

**Rule 3. Attendance at Closed Sessions.** The Co-Chairs, or their designees, shall attend closed sessions unless it is necessary to excuse them. Only such additional staff shall attend as are necessary and then only if the legal privileges of confidentiality obtained in an executive session are not waived.

**Rule 4. Reports from Closed Session.** It is the policy of the Port Security Committees to inform the public of action taken in closed session to the greatest extent possible. It is recognized, however, that the need for confidentiality is inherent in closed sessions and that certain matters if revealed may be a detriment to the results desired.

Reports from closed sessions, when permissible, shall be made by Co-Chairs or such other representative as designated by the Executive Subcommittee. Such designated person is the only individual authorized to make public statements concerning the closed session.

**Rule 5. Record of Disclosure of Security Sensitive Information.** The Co-Chairs shall assure that appropriate records are retained regarding the disclosure of SSI on a need to know basis, the specific Port Security Committee members to whom the information was disclosed, and the date.

## **Rules for Classified Sessions & Classified Information**

Classified Information must be protected under the rules governing it. Those rules shall be adhered to in all respects during classified sessions of the Port Security Committee. To the extent practicable, the rules outlined in section 2351 shall also be adhered to.

---

## **Rules for Commercially Sensitive Information**

Commercially Sensitive Information must also be protected. In all cases, Commercially Sensitive Information shall be treated in similar fashion to Security Sensitive Information and the rules outlined in section 2351 shall be adhered to.

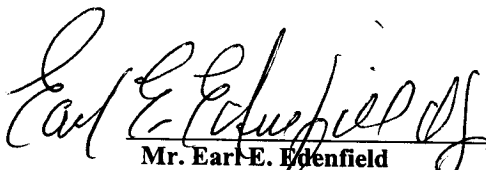
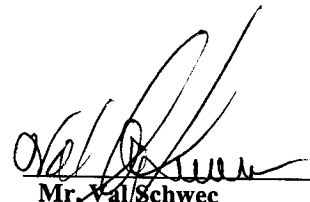
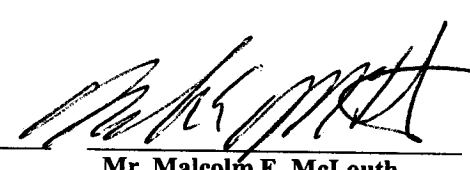
## **Rules for Proprietary Information**

Proprietary Information must also be protected. In all cases, Proprietary Information shall be treated in similar fashion to Security Sensitive Information and the rules outlined in section 2351 shall be adhered to.

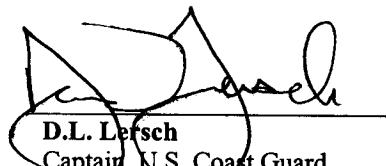
## **Amending The Charter**

This charter may be amended at any time by the Port Security Committee Co-Chairs. Recommendations to the Co-Chairs for changes to this charter may be made only with the approval of two-thirds of the Executive Subcommittee members.

Done, this 21<sup>st</sup> Day of October 2003, at the City of Jacksonville, Florida.

		
<b>Mr. Earl E. Edenfield</b> President, Jacksonville Marine Transportation Exchange	<b>Mr. Val Schwec</b> General Manager, Nassau Terminals	<b>Mr. Malcolm E. McLouth</b> Executive Director, Canaveral Port Authority

Accepted by the Federal Maritime Security Coordinator this 21<sup>st</sup> Day of October 2003, at the City of Jacksonville, Florida.

  
**D.L. Lersch**  
Captain, U.S. Coast Guard  
Federal Maritime  
Security Coordinator

## Appendix 9800 Glossary of Terms

This appendix is a glossary to terms commonly used throughout the Area Maritime Security Plan.

<b><u>Term</u></b>	<b><u>Definition</u></b>
<b>Absconder</b>	An inadmissible Crewmember that gains or attempts to gain illegal entry into the United States.
<b>Actionable Intelligence</b>	The collection, processing, analysis, and production and dissemination of intelligence to operational commanders with reasonable expectations that decisions will be made to take actions with resources available. Intelligence information that is directly useful to customers without having to go through the full intelligence production process. Similar to very real-time tactical intelligence.
<b>AIS</b>	Automatic Identification System: A shipboard broadcast system, which acts as a transponder, providing positional and other information to a remote receiving station.
<b>Alien</b> (also Migrant)	Any person not a citizen or national of the U.S. Individual aliens encountered by Coast Guard personnel will likely fall into one of the following categories: (1) Immigrants – those aliens coming to the U.S. to reside permanently. They may be entering for the first time or they may be alien residents of the U.S. who are returning from a temporary absence. (2) Non-immigrants – aliens seeking to enter the U.S. for a temporary period (e.g., business or vacation travel) or any person not a citizen or permanent resident of the U.S. (3) Illegal Entrants – those aliens who have entered the U.S. in such a manner as to avoid inspection. (4) Undocumented Migrants – those aliens attempting to illegally gain entry into a country without the required travel document(s) needed for admission.
<b>AMS</b>	Area Maritime Security
<b>AMS Assessment</b>	An analysis that examines and evaluates the infrastructure and operations of a port, taking into account possible threats, vulnerabilities, existing protective measures, procedures, and operations.
<b>Anchorage Surveys</b>	Waterborne harbor patrol to monitor anchorages used during military outload operations. Includes load line patrols, observations of vessel bunkering and lightering, and other patrols to prevent blockage or closure of the port.
<b>ANT</b>	Aids to Navigation Team
<b>ANVM</b>	Advance Notice of Vessel Movements: Vessels not meeting the ISM Code after June 30, 2002, will not be allowed to enter U.S. Ports until they can provide evidence of a fully implemented Safety Management System.
<b>AOR</b>	Area of Responsibility: A Coast Guard area, district, marine inspection zone or COTP zone described in 33 CFR 3.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-1
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

**Area Maritime Security Committee** A committee established under the direction of the COTP that assists in the development, review, and update of the Area Maritime Security Plan for a COTP geographic area of responsibility. The Committee functions under a charter and comprises at least seven members with five or more years of experience in maritime security operations. Additional responsibilities of the Committee include identification of critical port infrastructure and operations; identification of risks to the port area; determination of mitigation strategies and implementation methods; and assisting in communication of threats and changes in MARSEC levels and dissemination of appropriate security information to port stakeholders.

**Armed Vessel** Armed vessels are required for a number of USCG MHS activities. As a minimum, CG vessels shall have an M-16 or shotgun with copper sabot slugs and be adequately crewed with personnel trained and qualified on the carried weapons to be considered armed. The desired standard for “armed vessels” includes a mounted automatic firing weapon or weapons (i.e., 7.62 MM machine gun or Lietner-Wise modified M-16 rifle) in addition to carrying an M-16 rifle or shotgun. Until the USCG is adequately resourced, the requirement for the mounted weapons may be waived by the officer exercising COTP authority or Group Commander. Other law enforcement agency vessels and DoD vessels may be considered armed vessels when carrying weapons (sidearm, shoulder fired, or mounted) consistent with their organization/training, provided they have the legal authority to engage in the enforcement activity.

**Arrest** The seizure and taking into custody of a person, believed to have committed a crime, that occurs by the use of physical force or display of official authority, to which the person submits.

**Assault** Any willful attempt or threat to inflict injury upon the person of another, when coupled with an apparent present ability to do so, and any intentional display of force such as would give the victim reason to fear or expect immediate bodily harm. Physical contact is not required for an assault to have occurred (e.g., an individual points a firearm at another or attempts to stab another but misses).

**AT/FP** Antiterrorism/Force Protection: Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. Also called AT.

**Baseline** The line defining the shoreward extent of the territorial sea of the United States drawn according to principles, as recognized by the United States, of the Convention on the Territorial Sea and the Contiguous Zone. Normally, the territorial sea baseline is the mean low water line along the coast of the United States.

**Bioterrorism** The unlawful release of biologic agents or toxins with the intent to intimidate or coerce a government or civilian population to further political or social objectives. Humans, animals, and plants are often targets. 2. Use of microorganisms or toxins to kill or sicken people, animals or plants. The main difference between biological terrorism and conventional terrorism

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-2
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------



(i.e. bombs, hijackings, etc.) is the duration from the time of attack to the presentation of victims of the attack. Depending on the agent, the incubation period can be up to 60 days. It is highly probable that hospitals, not traditional first responders, will be the first to recognize a bioterrorism event secondary to the unfolding epidemiology and gradual increase in attack rates of a communicable agent.

**Breach of Security**

An incident, that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

**C2**

Command and Control: The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communication, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

**C4ISR**

Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance

**CBRNE**

Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive

**CDC**

Certain Dangerous Cargo: Includes any of the following:

- (1) Division 1.1 or 1.2 explosives as defined in 49 Code of Federal Regulations (CFR) 173.50
- (2) Division 1.5D blasting agents for which a permit is required under 49 CFR 176.415 or, for which a permit is required as a condition of a Research and Special Programs Administration exemption.
- (3) Division 2.3 "poisonous gas," as listed in 49 CFR 172.101 that is also a "material poisonous by inhalation" as defined in 49 CFR 171.8, and that is in a quantity in excess of 1 metric ton per vessel.
- (4) Division 5.1 oxidizing materials for which a permit is required under 49 CFR 176.415 or for which a permit is required as a condition of a Research and Special Programs Administration exemption.
- (5) A liquid material that has a primary or subsidiary classification of Division 6.1 "poisonous material" as listed in 49 CFR 172.101 that is also a "material poisonous by inhalation," as defined in 49 CFR 171.8 and that is in a bulk packaging, or that is in a quantity in excess of 20 metric tons per vessel when not in a bulk packaging.
- (6) Class 7, "highway route controlled quantity" radioactive material or "fissile material, controlled shipment," as defined in 49 CFR 173.403.
- (7) Bulk liquefied chlorine gas and Bulk liquefied gas cargo that is flammable and/or toxic and carried under 46 CFR 154.7.
- (8) The following bulk liquids: (i) Acetone cyanohydrin, (ii) Allyl alcohol, (iii) Chlorosulfonic acid, (iv) Crotonaldehyde, (v) Ethylene chlorohydrin, (vi) Ethylene dibromide, (vii) Methacrylonitrile, and (viii) Oleum(fuming sulfuric acid).

**CDP  
CEMP  
CERCLA**

Concept Deployment Plan  
Comprehensive Emergency Management Plan  
Comprehensive Environmental Response, Compensation, and Liability Act of 1980

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-3
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

<b>CFR</b>	Code of Federal Regulations: The compilation and codification of U.S. administrative law by subject matter arranged in numerical titles. The CFR is published officially by the federal government in volume form.
<b>CI</b>	Critical Infrastructure: The assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale.
<b>Classification</b>	The determination of the specific group or category a target belongs to (i.e., a fishing vessel, merchant vessel, naval vessel, yola). The determination of the current activity of a target is also an element of this function (e.g., a vessel dead in the water, fishing, smuggling visible contraband/undocumented migrants).
<b>Coastal Approaches Layer</b>	The waters from the U.S. Baseline (line of demarcation) seaward to 24 NM. This layer may extend to 50 NM, as necessary, for significant or designated Port Approaches (e.g., Tier 1 Ports) directly to the recognized U.S. territorial sea, from baseline seaward to 12 NM. The United States exercises Coastal State jurisdiction in this region.
<b>Coastal State</b>	A nation bordering ocean waters that has the authority under international law to exercise various degrees of sovereignty over the immediately adjacent ocean waters.
<b>Coastal State Authorization</b>	Permission from the coastal State to board and/or take actions in coastal State waters. Coastal State authorization is obtained through a special arrangement between the U.S. and the coastal State. The specific terms of the authorization determine exactly what action (e.g., entry, pursuit, patrol, boarding, search, detention, arrest, and/or seizure) the Coast Guard may take.
<b>Combined Operations</b>	Law enforcement or military operations between one or more U.S. forces or law enforcement agencies and the forces or law enforcement agencies of one or more allied nations in pursuit of common objectives.
<b>Concurrent Jurisdiction</b>	Jurisdiction over a location, vessel and/or persons that is shared by more than one sovereign. In U.S. navigable waters that are also within state jurisdiction, the U.S. and its states have concurrent jurisdiction over persons and vessels located therein.
<b>Consensual Boarding</b>	A boarding conducted solely with the consent of the master/person in charge of a vessel not subject to the jurisdiction of the U.S. Such boardings are non-jurisdictional in nature; no enforcement action whatever (e.g., seizure, arrest) may be taken while aboard a vessel solely on a consensual basis.
<b>Consequence</b>	The estimation of adverse effect from the target/attack scenario; an important consideration in risk evaluation and security planning.
<b>Consequence Management</b>	Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.
<b>Constructive Presence</b>	Under international law, the right of a coastal State to exercise jurisdiction

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-4
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

over a foreign-flag vessel (mother ship) that remains outside coastal State jurisdiction but uses its boat or another ship (contact boat) to commit offenses in violation of coastal State law within a maritime area over which that the coastal State exercises jurisdiction. In order to exercise jurisdiction over a mother ship located seaward of coastal State waters, the contact vessel must be physically present in coastal State waters or be subject to coastal State jurisdiction under the doctrine of hot pursuit. Once pursuit of the mother ship has legitimately commenced, it may proceed until it ceases to be continuous or until the mother ship enters foreign territorial waters. Cases potentially involving the doctrine of constructive presence can be complex and should be quickly referred to higher authority.

### **Contiguous Zone**

For the purpose of determining jurisdiction over location and interpreting international law, the waters within the belt adjacent to and seaward of the territorial sea and extending to 24 NM from the baseline (i.e., between 12 NM and 24 NM), but in no case extending within the territorial seas of another nation. For the purpose of determining the application of substantive law under the Federal Water Pollution Control Act and 19 USC, the waters within the belt 9 NM wide that is adjacent to and seaward of the 3 NM territorial sea (i.e., between 3 NM and 12 NM). (Source: MLEM)

(1) A maritime zone adjacent to the territorial sea that may not extend beyond 24 nautical miles (NM) from the baselines from which the breadth of the territorial sea is measured. Within the contiguous zone the coastal state may exercise the control necessary to prevent and punish infringement of its customs, fiscal, immigration, or sanitary laws and regulations within its territory or territorial sea. In all other respects the contiguous zone is an area subject to high seas freedom of navigation, over flight, and related freedoms, such as the conduct of military exercises.

(2) The zone of the ocean extending 3-12 NM from the US coastline. (Source: DOD Joint Pub 1-02) Contraband Any property that is unlawful to produce or possess. Also, goods exported from or imported into a nation against its laws.

### **Contraband Detection Activities**

The use of organic, mechanical or chemical devices that sample or examine the air or physical surfaces to detect the presence of contraband (e.g., cocaine, heroin, marijuana, explosives, weapons). CDA include, but are not limited to, the use of IONSCAN, CINDI, dogs, chemical reagent sprays, narcotics testing kits, and magnetometers.

### **COOP**

Continuity Of Operations Plan: The capability of a USCG Component to continue mission-essential functions without unacceptable interruption. COOP planning includes preparatory measures, response actions, and restoration activities planned or taken to ensure continuation of these functions to maintain military effectiveness, readiness, and survivability.

### **COP**

Common Operational Picture: A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness.

### **COTP**

Captain of the Port: The Coast Guard officer designated by the Commandant, U.S. Coast Guard, to direct Coast Guard law enforcement activities within a designated area of responsibility. A Captain of the Port

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-5
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

enforces regulations for the protection and security of vessels, harbors, and waterfront facilities; anchorages; bridges; safety and security zones; and ports and waterways. When designated by the MDZ Maritime Defense Commander (MARDEFCOM – Coast Guard District Commander MDZ designation), the COTP may serve as the Harbor Defense Commander (HDC).

<b>Counterterrorism</b>	The full range of activities directed against terrorism, including preventive, deterrent, response and crisis management efforts. Source: (U.S. Government Interagency Domestic Terrorism Concept of Operations Plan of 22 February 2001, Appendix B) Offensive measures taken to prevent, deter, and respond to terrorism. (Source: DOD Joint Pub 1-02)
<b>Crewmember</b>	Any person or persons serving in a capacity required for normal operation and service onboard a vessel. See High-Risk Detain Onboard Crewmember.
<b>Critical Assets</b>	Any facility, equipment, service or resource considered essential to DOD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration.
<b>CS</b>	Civil Support: Department of Defense support to U.S. civil authorities for domestic emergencies, and for designated law enforcement and other activities.
<b>CSG</b>	Counterterrorism Security Group
<b>CSO</b>	Company Security Officer: The person designated by the Company as responsible for the security of the vessel or OSC facility, including implementation and maintenance of the vessel or OSC facility security plan, and for liaison with their respective vessel or facility security officer and the Coast Guard.
<b>Customs Border Search</b>	A special type of search, conducted pursuant to customs authority, of a vessel and persons onboard at the U.S. border (or functional equivalent of the border) to enforce U.S. customs laws.
<b>Customs Waters</b>	For the U.S., generally those waters shoreward of a line drawn 12 NM from the baseline (including territorial sea and internal waters with ready access to the sea). For foreign flag vessels, customs waters of the U.S. may be extended beyond 12 NM by special arrangements (including treaties) between the U.S. and the vessel's flag State.
<b>Dangerous Substances and Devices</b>	Any material, substances, or item that reasonably has the potential to cause a transportation security incident.
<b>Deadly Force</b>	Any force that is likely to cause death or serious physical injury.
<b>Deserter</b>	A crewmember that is authorized by the CBP to enter but upon entry remains illegally in the United States.
<b>Detection</b>	The initial acquisition of a target by a sensor.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-6
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

**Detention** The act of keeping back, restraining, or withholding a person or property for a temporary, reasonable period of time for the purpose of inspection, investigation, or search when such act does not amount to an arrest or property seizure.

**DHS** Department of Homeland Security: The Homeland Security Act of 2002 established the Department of Homeland Security whose primary mission is to prevent, protect against, and respond to acts of terrorism on our soil.

**Disabling Fire** Disabling fire is the firing of ordnance at a vessel with the intent to disable, with minimum injury to personnel or damage to the vessel. Disabling fire as practiced by the Coast Guard does not constitute the use of deadly force. Such fire is a special method of stopping a vessel.

**Documented Vessel** A vessel documented under U.S. law (46 USC; 46 CFR, Subpart 67) and issued a Certificate of Documentation by the Coast Guard.

**DOD** Department of Defense

**DOD-Established Waterfront Terminals** A military-owned and Military Transportation Management Command (MTMC)-operated water terminal that provides regular terminal services, such as receipt, processing, staging, loading and unloading of DOD cargo.

**DOS** Declaration of Security: An agreement executed between the responsible Vessel and Facility Security Officer, or between Vessel Security Officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively.

**EEZ** Exclusive Economic Zone: For the purpose of determining jurisdiction over location and interpreting international law, the zone of waters beyond and adjacent to the territorial sea not extending beyond 200 NM from the baseline. For MSFCMA purposes, the inner boundary of the EEZ is the seaward limit of U.S. states and territory jurisdiction (i.e., 3 NM for most areas; 9 NM for Texas, the Gulf Coast of Florida, and Puerto Rico.) (Source: MLEM). A maritime zone adjacent to the territorial sea that may not extend beyond 200 nautical miles from the baselines from which the breadth of the territorial sea is measured. Within the EEZ, the coastal state has sovereign rights for the purpose of exploring, exploiting, conserving, and managing natural resources, both living and nonliving, of the seabed, subsoil, and the subjacent waters and, with regard to other activities, for the economic exploitation and exploration of the zone (e.g., the production of energy from the water, currents, and winds). Within the EEZ, the coastal state has jurisdiction with regard to establishing and using artificial islands, installations, and structures having economic purposes as well as for marine scientific research and the protection and preservation of the marine environment. Other states may, however, exercise traditional high seas freedoms of navigation, over flight, and related freedoms, such as conducting military exercises in the EEZ. (Source: DOD Joint Pub 1-02)

**Facility Security** A self analysis that examines and evaluates the infrastructure

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-7
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

<b>Assessment</b>	and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.
<b>FBI</b>	Federal Bureau of Investigation: The FBI's duties include protecting the U.S. from terrorist attacks, from foreign intelligence operations, and from cyber-based attacks and high-technology crimes; combating public corruption at all levels; protecting civil rights; combating international and national organized crime, major white-collar crime, and significant violent crime; supporting our law enforcement and intelligence partners; and upgrading FBI technology.
<b>FDEC</b>	Flight Deck Equipped Cutter
<b>Federal Register</b>	A daily publication in which U.S. administrative agencies publish both proposed regulations for public comment and final regulations.
<b>Felony</b>	A criminal offense punishable by death or imprisonment for more than one year.
<b>FEMA</b>	Federal Emergency Management Agency: FEMA is an independent federal agency with more than 2,600 full time employees working at FEMA headquarters in Washington D.C., at regional and area offices across the country, at the Mount Weather Emergency Operations Center, and at the FEMA training center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available to help out after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system. These partners include state and local emergency management agencies, 27 federal agencies and American Red Cross.
<b>Flag State</b>	The vessel claims the nationality of that nation and that nation exercises its jurisdiction and control in administrative, technical, and social matters over the vessel.
<b>Flag State Authorization</b>	Flag State authorization is permission from the flag State of a vessel to board and/or take enforcement actions with respect to that vessel. Flag State authorization is obtained through a special arrangement between the U.S. and the flag State. The specific terms of the authorization determine exactly what enforcement action (e.g., boarding, search, detention, arrest, and/or seizure) the Coast Guard may take with respect to the foreign vessel.
<b>FMSC</b>	Federal Maritime Security Coordinator: As stipulated in the Maritime Security Act of 2002, the Secretary will predesignate a Coast Guard official to serve as the FMSC in each area to develop an area maritime security plan and coordinate actions under the National Transportation Security Plan. (Source: Maritime Strategy for Homeland Security Pub 3-01). The National Maritime Transportation Security Plan, required by the MTSA, must designate areas for which Area Maritime Transportation Security Plans are required to be prepared and designate a Coast Guard official who shall be the Federal Maritime Security Coordinator for each such area. The Coast Guard designated the Captain of the Port, in 33 CFR 103.200, to be the FMSC for their respective COTP zones including all ports and areas located

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-8
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

therein, for the purposes of coordinating area maritime security activities. The FMSC is authorized to establish, convene, and direct the Area Maritime Security Committee (AMS); appoint members to the AMS Committee; develop and maintain, in coordination with AMS Committee, the AMS Plan; and implement and exercise the AMS Plan. (Source: MTSA [Public Law 107-295] Implementing Regulations 33 CFR 103.200)

**Force Majeure**

Under international law, the right of protection of a vessel forced into coastal State waters by virtue of distress that normally exempts it from coastal State jurisdiction for a reasonable period of time necessary to remedy such distress.

**Force Protection**

A security program designed to protect Service members, civilian employees, family members, facilities, and equipment in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

**Foreign Flag Vessel**

Foreign flag vessels are all seagoing vessels except U.S. vessels, vessels without nationality, and vessels assimilated to a vessel without nationality. (Source: MLEM) A vessel of foreign registry or a vessel operated under the authority of a country, except the U.S., that is engaged in commerce. (Source: MTSA)

**Foreign Layer**

Consists of foreign territory, ports of departure, and foreign territorial seas. Although this region lies within foreign jurisdiction, activities including International Maritime Organization (IMO) initiatives, Port State inspections, attachés/liaison officers, and cooperative Port/Flag State bilateral agreements can contribute significantly to maritime security.

**FOSC**

Federal On Scene Coordinator

**FSD**

Federal Security Director

**FSO**

Facility Security Officer: The person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers.

**FVI**

Foreign Vessel Inspection

**GMDSS**

Global Maritime Distress and Safety System: applies system automation techniques to the traditional maritime VHF, MF, and HF bands, which previously required a continuous listening watch. It incorporates the INMARSAT and the EPIRB satellite systems to improve the reliability and effectiveness of the distress and safety system on a global basis. GMDSS also provides for the timely dissemination of maritime safety information, including navigational and meteorological warnings and weather forecasts.

**Guiding Principles**

Describe overarching considerations that apply to the full spectrum of supporting objectives and performance standards.

**HDPAS**

High Density Population Areas (See Heavily Populated Area.)

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-9
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------



**Heavily Populated Area For Maritime Application** Cities with a population of more than 100,000 people.

**High-Risk Detain Onboard Crewmember (High-Risk Crewmember)** A Crewmember that meets both of the following criteria:

- The crewmember has been denied entry into the United States by the CBP.
- The crewmember meets the security risk criteria established by U.S. immigration authorities.

**High Seas Layer** Extends from the limit of the Maritime Approaches to foreign territorial seas. Jurisdiction is generally dependent on vessel nationality.

**HIV** High Interest Vessel: A commercial vessel intending to enter a U.S. port that may pose a high relative security risk to the port.

**HLD** Homeland Defense: The protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States. In understanding the difference between homeland security and homeland defense, it is important to understand that U.S. Northern Command is a military organization whose operations within the United States are governed by law, including the Posse Comitatus Act that prohibits direct military involvement in law enforcement activities. Thus, its missions are limited to military homeland defense and civil support to lead federal agencies.

**HLS** Homeland Security: A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

**HLSA 2002** Homeland Security Act of 2002

**Hot Pursuit** The pursuit of a foreign vessel on the high seas following a violation of law of the pursuing state committed by the vessel within a maritime area over which the state exercises jurisdiction, provided that the vessel evades boarding within the jurisdiction, and that the pursuit is continuous and uninterrupted. The right of hot pursuit must be exercised by a warship, military aircraft, or other authorized vessel or aircraft in government service of a coastal State. The right of hot pursuit ceases as soon as the pursued vessel enters the territorial seas of another coastal State.

**HSPD** Homeland Security Presidential Directive: Homeland Security Presidential Directive that shall record and communicate presidential decisions about the homeland security policies of the United States.

**HVA** High Value Asset: Any landside or waterside asset that is of high value. HVA may include military and commercial vessels, waterfront facilities, military facilities, submarines, or commercial vessels carrying CDC.

**HVU** High Value Unit: USN/NATO Aircraft Carriers; Submarines; LPDS, LHAS, LHDS, AND LSDS fully loaded with USMC contingent; and Military Sealift Command (MSC) Sealift / Pre-Positioned (PREPO) vessels carrying ammunition or other critical cargo.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-10
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



<b>ICS</b>	Incident Command System: Used to manage an emergency incident or a non-emergency event. It can be used for both small and large situations. The system has considerable internal flexibility and can grow or shrink to meet differing needs. This makes it a very cost-effective and efficient management system that can be applied to a wide variety of emergency and non-emergency situations. HLS Directive 5 requires the use of NIMS.
<b>Identification</b>	The determination of a characteristic that uniquely differentiates a particular vessel from others in the same classification category (i.e., the name and/or registration numbers of a vessel).
<b>IDS</b>	Integrated Deepwater System: Multi-year program to recapitalize, update, and improve the capabilities of the U.S. Coast Guard's current fleet of ships and aircraft, providing the best mix of aircraft, cutters, sensors, communications and logistics capabilities. At full implementation, Deepwater will comprise three classes of new cutters and their associated small boats, a new fixed wing manned aircraft fleet, a combination of new and upgraded helicopters, and both cutterbased and land-based UAVs. All these assets will be linked with interoperable C4ISR systems, and will be supported by an integrated logistics regime. Deepwater missions are performed close to shore or far out to sea and involve either extended on scene presence, long transit distances, or forward deployment, and exceed the operating capabilities of shorebased small boats. Deepwater forces significantly contribute to the homeland security by providing a capability to detect, intercept and interdict potential threats on the high seas,
<b>ILO</b>	International Labor Organization: A UN-specialized agency which seeks to promote social justice and internationally recognized rights, create employment opportunities and improve working conditions around the world
<b>IMO</b>	International Maritime Organization: A London- based United Nations organization whose decisions have treaty status in the U.S. and most of the world. The purposes of the Organization, as summarized by Article 1(a) of the Convention, are "to provide machinery for cooperation among Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation and prevention and control of marine pollution from ships".
<b>Innocent Passage</b>	Under international law, the right of non-interference for a vessel transiting inbound, outbound or through a foreign territorial sea, provided the vessel's passage is innocent.
<b>Inspection</b>	An examination of government licensees, heavily regulated businesses or activities for compliance with government regulations.
<b>Internal Waters</b>	For the U.S., the waters shoreward of the baseline, including all waters on the U.S. side of the international boundary of the Great Lakes. For any other nation, the waters shoreward of its baseline as recognized by the U.S. International Waters The waters seaward of the outer limit of the territorial sea of any nation, but encompassing the high seas, EEZ, and contiguous

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-11
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

zones.

**Intrusive Search**

A quest for evidence that may require the destruction or permanent alteration of personal property to complete the search.

**ISI**

Initial Safety Inspection: A protective sweep of a vessel for the safety of the boarding team. There are two levels of initial safety inspection: (1) basic and (2) extended.

**ISPS**

Code International Ship and Port Facility Security Code: As incorporated into SOLAS.

**JHOC**

Joint Harbor Operations Center: A combined Coast Guard and Navy Operations Center that coordinates all port-security measures within a port to keep warships and commercial shipping safe from attack. It acts as a clearinghouse for emergency response to possible threats.

**Joint Operations**

A general term applied to law enforcement actions between two or more U.S. law enforcement agencies, or law enforcement actions involving one or more U.S. law enforcement agencies and one or more of the U.S. Armed Services. (Source MLEM) A general term to describe military actions conducted by joint forces or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces.

**Jurisdiction**

The government's right to exercise legal authority over its persons, vessels, and territory. Within the context of MLE, jurisdiction is comprised of three elements: substantive law, vessel status/flag, and location.

**KA**

Key Assets (See MCI/KA.)

**Key Command Posts**

Command posts critical to the command and control of security/consequence management operations.

**Key Port Areas**

Areas within ports or along navigable waterways where heavily populated areas, DOD assets, choke points, or MCI/KA would be vulnerable to attacks.

**Layered Defense**

A subset of layered maritime security. A system of multiple lines of defense with the specific objective of protection.

**Layered Maritime Security**

A system of diverse activities designed to provide multiple opportunities to prevent successful terrorist attacks.

**LEDET**

Law Enforcement Detachment: A deployable, small team of U.S. Coast Guard personnel who principally conduct maritime law enforcement tasking from Coast Guard units (both afloat and ashore), U.S. Navy ships, and selected foreign navy ships.

**LFA**

Lead Federal Agency: The agency designated by the President to lead and coordinate the overall Federal response is referred to as the LFA and is determined by the type of emergency. In general, an LFA establishes operational structures and procedures to assemble and work with agencies providing direct support to the LFA in order to provide an initial assessment of the situation; develop an action plan; monitor and update operational

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-12
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

priorities; and ensure each agency exercises its concurrent and distinct authorities under U.S. law and supports the LFA in carrying out the president's relevant policy. Specific responsibilities of an LFA vary according to the agency's unique statutory authorities.

#### **Major Initiatives**

The executable initiatives and activities that describe the highlevel mechanism for achieving the strategic and supporting objectives via the strategy elements.

#### **Manifest**

A collection of forms required for presentation upon a vessel's arrival or departure in/from the United States. Typically these include, but are not limited to, Form I-418 (Crew List), Form I-92 (Vessel Report), Form I-94 (Arrival/Departure Record), and Form I-95 (Conditional Landing Permit).

#### **Marine Environment**

The navigable waters of the United States and the land and resources therein and thereunder; the waters and fishery resources of any area over which the United States asserts exclusive fishery management authority; the seabed and subsoil of the Outer Continental Shelf of the United States, the resources thereof and the waters superadjacent thereto; and the recreational, economic, and scenic values of such waters and resources.

#### **Maritime Approaches**

Layer Extends from the Coastal Approaches seaward to the Oceanic Layer. It contains the U.S. Exclusive Economic Zone in its entirety. Jurisdiction in this region largely depends upon vessel registry.

#### **MARSEC**

Maritime Security:

- MARSEC 1 – New normalcy; minimum measures that have to be maintained at all times.
- MARSEC 2 – Heightened threat of a transportation security incident; set for as long as threat lasts
- MARSEC 3 – Transportation security incident probable or imminent; envisioned to be set for shorter period of time.

#### **MARSEC Directive**

An instruction issued by the Commandant, or his/her delegate, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.

#### **MARSEC Level**

The level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

#### **MCI/KA**

Maritime Critical Infrastructure/Key Assets: Facilities, structures, systems, assets or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health, or safety of the port.

#### **MDA**

Maritime Domain Awareness: Comprehensive information, intelligence, and knowledge of all relevant entities within the U.S. maritime domain – and their respective activities – that could affect America's security, safety, economy, or environment. MDA provides operational forces with an understanding of what is normal in order to increase the likelihood of

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-13
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

spotting the abnormal or unusual when it occurs.

**MDIS**

Maritime Domain Information System

**MHD**

Maritime Homeland Defense

**MHD Operations**

Operations to counter a maritime threat where the department of defense would take the lead, acting through NORTHCOM and NAVNORTH, in defending U.S. citizens and territory, supported by other agencies.

**MHS**

Maritime Homeland Security: MHS is a federal law enforcement mission carried out by domestic law enforcement authorities, including the Coast Guard, and shall be conducted in accordance with settled law enforcement procedures, The Maritime Law Enforcement Manual (COMDTINST M16247.1 (SERIES)) And other applicable law enforcement policies. DOD personnel may assist non-DOD law enforcement authorities with MHS law enforcement missions in accordance with Federal law and applicable DOD and Coast Guard regulations and policies. MHS does not include the physical security of Coast Guard units and property, which shall be conducted in accordance with the Physical Security and Force Protection Manual, COMDTINST M5530.1C.

**Migrant**

See Alien.

**Milestones**

Describe the time -phased projects to accomplish the major initiatives.

**Military Essential Cargo** Military supplies and equipment essential to the accomplishment of military strategic or operational objectives.

**Military Essential  
Transportation Facilities**

See Military Essential Waterfront Facilities.

**Military Essential  
Transportation Routes**

For maritime application, rail and road bridges across navigable waterways that are essential to moving military supplies, equipment and/or personnel into or out of a port.

**Military Essential  
Waterfront Facilities**

Commercial or military waterfront facilities used to out load supplies and equipment essential to the accomplishment of military strategic objectives.

**Military Essential  
Waterways**

A waterway used by military vessels or vessels carrying military essential cargo or personnel.

**MIO**

Maritime Interception Operations

**Misdemeanor**

Any crime other than a felony.

**Mission**

Provides a broad statement describing the reason for the organization's existence and long-term outcomes. (Source: MHS Strategy Deployment Plan)

(1) The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.

(2) In common usage, especially when applied to lower military units, a

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-14
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

duty assigned to an individual or unit; a task. (Source: DOD Joint Pub 1-02)

<b>MLE</b>	Maritime Law Enforcement
<b>MMRS</b>	Metropolitan Medical Management System
<b>Mobile Command And Control (C2) Assets</b>	Any mobile structure or system that can be used for command and control, such as a mobile incident command post, mobile command center, and the marine information for safety and law enforcement (MISLE) system.
<b>MOL</b>	Military Outload: Loading or unloading of military cargo or ammunition in support of actual or potential combat operations.
<b>MSD</b>	Marine Safety Detachment
<b>MSF</b>	Maritime Security Force: Twelve U.S. Navy mobile detachments provided for armed interdiction to protect deployed U.S. Navy ships, aircraft, and other DON units against terrorist attack in locations where U.S. shore infrastructure does not exist or requires augmentation. The MSF concept is built upon modular force elements capable of short duration tailored tasks as well as regional combatant commander-specified mission task. Detachments contain three boats with M60/50Cal/40MM weapons. Crew: 76 total. Boat Crews and 54 Security Personnel.
<b>MSO</b>	Marine Safety Office
<b>MSST</b>	Maritime Safety and Security Team: U.S. Coast Guard deployable unit established for PWCS activities in the port and coastal regions. These 106-person, 6-boat units are modeled after the Coast Guard's existing Port Security Units and Law Enforcement Detachments to provide a fast-deployment capability for PWCS.
<b>MTS</b>	Marine Transportation System: Consists of waterways, ports and intermodal connections, vessels, vehicles, and system users, as well as federal maritime navigation systems.
<b>MTSA 2002</b>	Maritime Transportation Security Act of 2002: Landmark legislation passed by the 107th Congress to increase the security efforts of the Coast Guard and other agencies in the U.S. Maritime Domain.
<b>MTS Infrastructure</b>	See Maritime Critical Infrastructure/Key Assets (MCI/KA).
<b>National Self-Defense</b>	The act of defending the United States, U.S. forces, and/or in certain circumstances, U.S. citizens and their property, U.S. commercial assets, or other non-designated U.S. forces, foreign nationals and their property, from a hostile act or hostile intent.
<b>NATO</b>	North Atlantic Treaty Organization
<b>Navigable Waters of the United States</b>	For the purpose of the Federal Water Pollution Control Act, those waters shoreward of 3 NM from the baseline, including internal waters

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-15
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

and all other waters subject to federal Constitutional authority. For all other purposes, those waters shoreward of 12 NM from the baseline, including internal waters subject to tidal influence and those waters not subject to tidal influence that are or have been used, or susceptible of use, as highways for substantial interstate or foreign commerce, or capable of improvement at a reasonable cost to serve as highways for substantial interstate or foreign commerce. Each Coast Guard District maintains a current list of navigable waters of the U.S. within that District.

**Neutralize  
NIC**

To render ineffective or unusable.  
National Incident Command: An organization activated by the Commandant or Area Commander that is functionally similar to the regional incident command in all aspects, but the complexity of the incident requires the direct involvement of the most senior Coast Guard Operational Commanders.

**NIMS**

National Incident Management System: A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State and local capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certifications; and the collection, tracking, and reporting of incident information and incident resources

**NM**

Nautical Mile

**NOA**

Notice of Arrival: Owners, agents, masters, operators, or persons in charge of vessels bound for U. S. ports must file a Notice of Arrival 96 hours before entering port.

**Non-Compliant Vessel**

A vessel subject to examination that refuses to heave to after being legally ordered to do so.

**Non-Deadly Force**

Any force other than deadly force.

**NPRN MOU**

National Port Readiness Network Memorandum of Understanding: To ensure military and commercial seaport readiness to support deployment of military personnel and cargo in the event of mobilization or national defense contingency through enhanced coordination and cooperation among affected organizations.

**NRP**

National Response Plan: A plan mandated by HSPD-5 that integrates Federal Government domestic awareness, prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.

**NSF**

National Strike Force: A U.S. Coast Guard capability composed of three mobile units established for rapid response to oil discharges and hazardous substance releases. With highly specialized equipment, NSF units support

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-16
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

Federal On-Scene Coordinators and Coast Guard incident commanders to reduce the environmental damage from oil discharges and hazardous substance releases. Since the NSF also has a CBRNE capability (that was used in the aftermath of the bioterrorism attacks on the U.S. Capital), the NSF has a major role in homeland security preparedness and recovery operations in the U.S. Maritime Domain.

#### NVPS

Naval Vessel Protection Zone: As described in 33CFR 165, Subpart G, A NVPZ is a 500-yard regulated area of water, including a 100-yard exclusion zone, surrounding large U.S. Naval Vessels, including MSC vessels, in effect at all times in the navigable waters of the U.S. (out to 3NM), whether the large naval vessel is underway, anchored, moored, or within a floating dry dock, except when the large naval vessel is moored within a restricted area or within a naval defensive sea area.

#### Oceanic Layer

Extends from the limit of the Maritime Approaches to foreign territorial seas. Jurisdiction is generally dependent on vessel nationality.

#### Oceanic Sector

Extends from the seaward limit of foreign territorial seas to a line 200 NM seaward of the U.S. baseline.

#### OCS

Outer Continental Shelf

#### Official Number

The serial number of a U.S. documented vessel as permanently issued on a Certificate of Documentation by the Coast Guard. Certain other vessels, which are not required by law to be numbered, have been marked with "unofficial identification numbers" (e.g., public vessels owned by the Maritime Administration have their number preceded by the letters MC, inspected inland tank barges have a six digit number issued by the Coast Guard and preceded by the letters "CG").

#### OPCON

Operational Control: The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives and giving authoritative direction over all aspects of law enforcement or military operations and joint training necessary to accomplish assigned missions. OPCON may be exercised at any echelon at or below the level of Area Commander, or combatant command for joint operations, and can be delegated or transferred. OPCON, in and of itself, does not include authoritative direction for logistics, administration, discipline, internal organization, or training. (Source: MLEM) Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-17
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. See also combatant command; combatant command (command authority); tactical control. (Source: DOD Joint Pub 1-02)

**Operational Concept** Summarizes the types and scope of operational activities and support required in addressing threats and vulnerabilities to meet the stated goals and objectives.

**Operational Function** Outreach/Partnering Establish and maintain partnerships with local, state, national and international agencies and industry to identify and implement best practices to mitigate security risks and strengthen security network while minimizing impact on commerce.

**PAWSS** Ports and Waterways Safety System: A U.S. Coast Guard project to provide an integrated system of vessel traffic centers, communications, information management capabilities, remote sensors, and associated facilities for vessel traffic management in selected U.S. ports and waterways to provide safe operations and protect the environmental. PAWSS capabilities can directly support Coast Guard maritime security operations for tasking such as surveillance, detection, and command and control.

**PDD** Presidential Decision Directive

**Physical Security** That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. *Or* Security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

**Port** A geographic area, either on a seacoast, lake, river or any other navigable body of water, which contains one or more publicly or privately owned terminals, piers, docks, or maritime facilities, which is commonly thought of as a port by other government maritime-related agencies. (Source: CG MDA Concept Deployment Plan) A defined geographical, political, or regional area in the Marine Transportation System that may be further defined by the Captain of the Port. (Source: Port Security Assessment team)

**Port Facilities and Services** (1) All port facilities for coastwise, intercoastal (except as to shipping between the U.S. ports on the Great Lakes), and overseas shipping, including but not limited to wharves, piers, sheds, warehouses, yards, docks, control towers, container freight stations, and port equipment, including harbor craft, cranes and straddle carriers; and (2) port services normally used in accomplishing the transfer or interchange of cargo and passengers between ocean-going vessels and other modes of transportation.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-18
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



<b>Port Layer</b>	Extends from navigable rivers, canals, and waters seaward to the U.S. Baseline. It also includes the nodes or points where the Marine Transportation System meets the air and land transportation systems.
<b>Port Security</b>	The safeguarding of vessels and critical assets within a port from internal threats such as destruction, loss, or injury from sabotage or other subversive acts, accidents, thefts, or other causes of a similar nature (see 50 U.S. Code [USC] 191, JCS Publication 1, and 33 CFR Part 6).
<b>Port Security Vessel Targeting Matrix</b>	A tool to assist operational commanders in identifying those arriving vessels that pose the highest relative security risks in their ports and in allocating their resources, including MSSTs, to reduce those risks. While the matrix highlights HIVs that must undergo security boardings, it also identifies other vessels for which other control measures, including boardings, may be indicated as additional or alternative means to address their specific security risks.
<b>Port State Control</b>	Inspection of foreign ships in national ports to verify that the condition of the ship and its equipment comply with the requirements of international regulations and that the ship is manned and operated in compliance with these rules.(IMO)
<b>Port State Control Boarding Matrix</b>	Boarding matrix that enables the Coast Guard to rationally and systematically determine the probable risk posed by non-U.S. ships calling at U.S. ports. The Matrix is used to decide which ships Port State Control Officers should board on any given day, in any given port. Points are assessed in each of the five columns and then summed for a total point score. This numerical score, along with other performance based factors, determines a ship's boarding priority. The Boarding Priority Matrix illustrates the priority categories and associated operational restrictions that may be imposed on ships by U.S. Coast Guard Captains of the Port.
<b>Positive Control Measures</b>	Where intelligence or other information indicates a possible internal threat to the vessel, COTPs may implement positive control measures intended to enhance the internal security of the vessel and to ensure that the vessel remains under the control of appropriate shipboard authorities (i.e., master and pilot), particularly while the vessel transits critical or vulnerable areas of the port. Such measures include security boardings, requiring the vessel to anchor offshore, directing the vessel to employ tugs, and requiring the vessel to embark private security personnel. Positive control measures requiring the employment of armed security to conduct onboard positive control operations may provide a visible deterrent to illicit activity, increase public confidence in the MTS, and may be tactically effective in reducing the risk that the vessel may be used as a weapon against critical infrastructure or other high-value targets. (Source: MLEM) Concurrent with or upon completion of a security boarding, armed boarding team members take up positions aboard the vessel to deter, detect, prevent, and respond to acts of terrorism and /or transportation security incidents. (Source: COMDT Message Terms of Reference for Maritime Homeland Security [Draft V8])
<b>Probable Cause</b>	The level of suspicion that would cause a reasonable and prudent person, given the overall circumstances, to believe a crime has been committed.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-19
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

Probable cause is a judgment call made by a law enforcement officer based on the totality of the circumstances, including the officer's training, experience, and analysis of the situation.

**Prosecution**

This activity involves intercepting or closing the distance to the TOIs in order to deliver end game capability that is mission and situation specific.

**PSA**

Port Security Assessment

**PSC**

Port Security Committee

**PWCS**

Ports Waterways & Coastal Security: Protect the U.S. Maritime Domain and the U.S. Marine Transportation System from internal and external threats, such as: destruction, loss, or injury from terrorism, sabotage or other Subversive acts.

- Deny their use and exploitation as a means for attacks on U.S. territory, population, and critical infrastructure.
- Prepare for and, in the event of attack or incident, conduct emergency response operations.
- When directed, as the supported or supporting commander, transition to and conduct military homeland defense operations.

**PWSA**

Ports and Waterways Safety Act

**Reasonable Suspicion**

The belief by a reasonable and prudent person based on facts, that something has happened (e.g., criminal activity is afoot or a particular condition exists). This is a comparatively low standard short of the probable cause threshold, But rising above the level of mere suspicion.

**Refugee**

An individual that has been determined by competent authority to be fleeing persecution or have a well-founded fear of persecution in their own country because of race, religion, nationality, membership in a particular social group or political opinion. This does not include individuals being protected while their asylum request is being reviewed. (Source: MLEM) A person who, by reason of real or imagined danger, has left their home country or country of their nationality and is unwilling or unable to return. See also dislocated civilian; displaced person; evacuee; expellee; stateless person. (Source: DOD Pub 1-02)

**Rescue 21**

The National Distress and Response System is the replacement communications and distress reporting system for the U.S. Coast Guard. Once fielded this new communications system will serve as the means for Coast Guard operational commanders to exercise command and control (C2) over Coast Guard all units conducting all missions along the 95,000-mile U.S. coastline out to 20 miles offshore, as well as, in the ports and interior waterways including the Great Lakes. Additionally, NDRS serves as the emergency reporting system for the public and commercial mariners for them to contact the Coast Guard if in distress.

**Response Force Deployment**

Deployment of force packages, including special operations teams, in response to PWCS incidents/events. Restricted areas The infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-20
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

of security protection. The entire facility maybe designated the restricted area, as long as the entire facility is provided the appropriate level of security.

## **RIC**

Regional Incident Command: An organization activated by the District Commander to ensure coordination for command, planning, and logistical matters. The need for a RIC may arise when there are multiple Coast Guard Incident Commanders and/or when there is heavy demand for COAST GUARD resources from other agencies such as FEMA or the EPA. The RIC will determine which critical resources are sent to which incident and determine priorities for their assignment.

## **Right of Approach**

Under international law, the right of warships and other duly authorized vessels or military aircraft in international waters to approach any vessel in international waters and to verify its nationality through questioning. The Right of Approach is closely linked to the Right of Visit.

## **Right of Visit**

Under international law, the right of warships and other duly authorized vessels or military aircraft in international waters to board a vessel of unknown nationality in order to determine its nationality, or to board any vessel suspected of engaging in piracy, slave trade or unauthorized broadcasting.

## **Risk**

Expected losses over time: Risk = Threat x Vulnerability x Consequence

**Threat:** Is a measure of the probability of an attack based on maritime domain awareness and intelligence.

**Vulnerability:** Is the conditional probability of success given that a threat scenario occurs. It evaluates the adequacy and effectiveness of safeguards (both existing and proposed)

**Consequence:** Is the estimation of adverse effect from the target/ attack scenario and is an important consideration in risk evaluation and security planning. (Source: Federal Register Vol. 68 No. 126, Page 39244)  
Probability and severity of loss linked to hazards. (Source: MLEM)  
A measure combining an undesirable event's frequency and consequence. (Source: Risk Based Decision Guide) The calculated probability of loss or damage to an asset based on its attractiveness, vulnerability, and threat environment. (Source: MSM Vol. VII [Draft Revision])

## **Safety Zone**

A designated water or shore area to which access is limited to persons, vehicles, vessels, or objects authorized by the COTP. It may be stationary and described by fixed limits or it may be described as a zone around a vessel in motion. A Safety Zone may be established by regulation under the authority of the Port and Waterways Safety Act (PWSA) (33 USC 1221) within which vessel traffic controls, and operating restrictions may be imposed. (Source: MSM Vol. VII [Draft Revision]) An area (land, sea, or air) reserved for noncomb at operations of friendly aircraft, surface ships, submarines, or ground forces. (Note: DOD does not use the word "submarines.") (Source: DOD Joint Pub 1-02)

## **SANS**

Ship Arrival Notification System: National Vessel Movement Center database used to collect and forward information to the intelligence community, marine safety offices and other authorities.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-21
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**SAR** Search and Rescue

**Screen** A reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present. (Source: CFR 101.105) A security element whose primary task is to observe, identify, and report information, and which only fights in selfprotection. (Source: DOD Joint Pub 1-02)

**Security** A condition that results from measures established to protect designated information, personnel, systems, components and equipment against hostile persons, acts, or influences. (Source: CG MDA Concept Deployment Plan)

- (1) Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness.
- (2) A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
- (3) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (Source: DOD Joint Pub 1-02)

**Security Audit** An evaluation of a vessel or facility security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party, intended to identify deficiencies, non-conformities and/or inadequacies that would render the assessment or plan insufficient.

**Security Boarding** An examination by an armed boarding team of a vessel (including the cargo, documentation, and persons on board) designated by the Captain of the Port (COTP), arriving or departing at a U.S. port, to deter acts of terrorism and/or transportation security incidents. COTPs may order a security boarding for vessels engaged in domestic operations if intelligence or other law enforcement information warrants.

**Security Inspection** A USCG inspection of a vessel or facility to verify compliance with its approved security plan.

**Security Spot Check** A USCG or multi-agency visit to a facility or vessel to verify compliance with all or part of its approved security plan for the current security condition.

**Security Survey** An on-scene examination and evaluation of the physical characteristics of a vessel or facility, and its security systems, processes, procedures, and personnel.

**Security Sweep** A walkthrough to visually inspect unrestricted areas to identify unattended packages, briefcases, or luggage and determine that all restricted areas are secure.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-22
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

<b>Security System</b>	A device or multiple devices designed, installed and operated to monitor, detect, observe or communicate about activity that may pose a security threat in a location or locations on a vessel or facility.
<b>Security Zone</b>	A designated areas of land, water, or land and water established for such time as the COTP deems necessary to prevent damage or injury to any vessel or waterfront facility, to safeguard ports, harbors, territories, or waters of the United States, or to secure the observance of the rights and obligations of the United States. (Source: 33 CFR Part 6) All areas of land or water which are so designated by the COTP for such time as deemed necessary to prevent damage or injury to any vessel or waterfront facility, to safeguard ports, harbors, bridges, territories, or waters of the United States or to secure the observance of the rights and obligations of the United States. (Source: MHS Strategy Deployment Plan)
<b>Self-Defense</b>	See Individual Self-Defense, National Self-Defense, or Unit Self-Defense.
<b>SIPRNET</b>	Secret Internet Protocol Router Network: Worldwide secret level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. (See also Defense Information Systems Network.)
<b>SIV</b>	Special Interest Vessel: A vessel (commercial, cargo, passenger, fishing and fisheries support; public and private yacht) that, due to country of registry (flag state), ownership, or charter, has been identified by the Executive Branch as a potential threat to national security while within U.S. ports, internal waters or territorial seas.
<b>SLOC</b>	Sea Lines of Communications
<b>SNO</b>	Statement of No Objection: The means by which a Coast Guard flag officer informs a subordinate commander that the flag officer does not object to the proposed use of the subordinate commander's lawful discretion and authority.
<b>SOLAS</b>	Safety of Life at Sea
<b>Special Deputy Marshal</b>	Armed and uniformed Coast Guard Boarding Officers specially deputized as Deputy U.S. Marshals for the purpose of conducting MHS law enforcement ashore include monitoring and ensuring the adequacy of facility security measures, augmenting facility security forces to man access control points, securing facility perimeters against intrusion, manning fixed weapons emplacements on piers and facilities to protect against waterside attack, and securing waterside access to critical infrastructure.
<b>SROE</b>	Standing Rules of Engagement : Guidance on the use of force for the accomplishment of non-law enforcement missions, unit self-defense, and national self-defense. SROE also establish fundamental policies and procedures governing action to be taken by U.S. force commanders during military operations and contingencies.
<b>SSI</b>	Sensitive Security Information: Information within the scope of 49 CFR Part

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-23
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

1520.

<b>Standards</b>	Designate expected levels of accomplishment and address performance levels (outcomes) for strategic and supporting objectives.
<b>State</b>	“State” as used herein has one of two meanings: a nation (as in flag or coastal State) or one of any of the fifty states of the U.S. This plan employs the term “State” to denote nations and “state” to indicate one of the fifty United States. Some statutes, such as the MSFCMA, define “state” to include certain U.S. territories or other possessions.
<b>Stateless Vessel</b>	See Vessel without Nationality.
<b>Stowaway</b>	Any person who is secreted on a ship, or in cargo which is subsequently loaded on the ship, without the consent of the ship’s owner or the master or any other responsible person and who is detected onboard the ship after it has departed from a port, or in the cargo while unloading it in the port of arrival. Also defined as an alien coming to the U.S. surreptitiously on an airplane or vessel without legal status for admission.
<b>Strategic Objectives</b>	Describe the desired end state focus of the organization, which can be implemented through activities and initiatives that address the mission.
<b>Strategic Sealift Vessel</b>	Common-user sealift asset of the MSC force, including fast sealift ships and pre-positioned ships. The normal peacetime force may be augmented by shipping from the Ready Reserve Fleet, The National Defense Reserve Fleet, and from U.S. and Allied Merchant Fleets.
<b>Strategy Elements</b>	Describe implementation strategies that cut across the strategic objectives and serve to guide resourcing and mission execution expectations.
<b>Supported Commander</b>	The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operational planning authority. In the context of joint operation planning, this term refers to the commander who prepares operations plans or operations orders in response to the requirements of the Chairman of the Joint Chiefs of Staff.
<b>Supporting Commander</b>	A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the designated combatant commands and Defense agencies as appropriate.
<b>Supporting Objectives</b>	The desired components of the end state that will drive the organization to achieve the established strategic objectives.
<b>Surveillance</b>	Employment of sensors, active or passive, to scan an area and detect targets. Modeled types of surveillance include, transit surveillance and patrol surveillance. (Source: MSMP) The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (Source: DOD Joint Pub 1-02) Includes all sources (inspections, intelligence, regulations, reporting, presence, participation, fixed/mobile sensors [equipment and/or personnel]. (Source: MHS Strategy Deployment Plan)

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-24
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

**Suspected Terrorist Activity**

Activities that meet the initial sorting criteria applicable in the area where the activities are detected.

**TACON**

Tactical Control: Command authority over assigned forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and usually local direction and control of movements and maneuvers necessary to accomplish assigned missions or tasks. TACON may be exercised by commanders at any echelon below the Area Commander level, or by combatant command for joint operations. TACON does not provide organizational authority or authoritative direction for administrative and logistics support; the parent unit continues to exercise those responsibilities unless otherwise directed. (Source: MLEM)

Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. When forces are transferred between combatant commands. The command relationship, the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (Source: DOD Joint Pub 1-02)

**TBD**

To Be Developed

**Territorial Sea (Foreign)**

The waters within the belt that is adjacent to the foreign nation's coast and whose breadth and baseline are recognized by the U.S.

**Territorial Sea (U.S.)**

The waters within the belt, 12 NM wide, that is adjacent to the coast of the U.S. and seaward of the baseline, for the following purposes:

- Determining jurisdiction over location.
- Interpreting international law.
- Determining the applicability of substantive laws within Subtitle II, 46 USC and the Ports and Waterways Safety Act, 33 USC 1221, and any regulations issued under the authority of these statutes.
- Determining the applicability of substantive laws within 18 USC
- Determining the applicability of substantive laws related to the special maritime and territorial jurisdiction of the U.S. as defined in 18 USC 7.

For the purpose of determining the applicability of substantive U.S. domestic laws not mentioned above, the territorial sea means the waters within the belt, 3 NM wide, that is adjacent to the coast of the U.S. and seaward of the baseline.

**Territorial Sea Baseline**

See Baseline.

**Terrorism**

The term "terrorism" has several definitions and varies depending on the context in which the term is employed. When using the term in the context of criminal investigations, Coast Guard personnel shall refer to the specific statute to ensure that the conduct under consideration meets the elements of the specific offense. For purposes of operations planning, terrorism means

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-25
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



any activity that involves an act that (I) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (II) is a violation of U.S. criminal law or of any state or other subdivision of the U.S.; and appears to be intended (I) to intimidate or coerce a civilian population; (II) to influence the policy of a government by intimidation or coercion; or (III) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

**Threat**

A measure of the likelihood of an attack based on maritime domain awareness and the existence of intelligence.

**TOI**

Target Of Interest: An object identified for mission prosecution as a result of classification based on characteristics, behavior or other identification.

**Transportation  
Infrastructure**

See MCI/KA.

**Transportation  
Security Incident**

A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

**UASI  
UNCLOS**

Urban Area Security Initiative  
United Nations Convention of the Law of the Sea

**Unified Command Post**

The location at which the primary unified command functions are executed as a team effort, allowing all agencies with responsibility for an incident to perform these functions without losing or abdicating agency authority, responsibility or accountability.

**U.S. Maritime Domain**

Encompasses all U.S. ports, inland waterways, harbors, navigable waters, Great Lakes, territorial seas, contiguous zone, customs waters, coastal seas, littoral areas, the U.S. exclusive economic zone, and oceanic regions of U.S. national interest, as well as the sea lanes to the U.S., U.S. maritime approaches, and the high seas surrounding America.

**Unified Command**

A command with a broad continuing mission under a single commander and composed of significant assigned components of two or more Military Departments, that is established and so designated by the President through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff.

**Unit Self-Defense**

The act of defending a particular unit of U.S. forces, and other U.S. forces in the vicinity, against a hostile act or hostile intent.

**Universal Crimes**

Under international law, crimes (i.e., piracy, slavery, and unauthorized broadcasting) subject to the jurisdiction of any nation.

**Urgent SAR**

In the context of mission priority, SAR can be considered in the context of defined SAR phases. For the purposes of Neptune Shield operations, urgent SAR equates to the definition for the distress phase: the phase that exists when grave or imminent danger requires immediate response to the threatened craft or person. In the context of resource availability, urgent SAR posture requires maintaining the minimum readiness to respond to SAR cases where an imminent threat to life exists.

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-26
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------



<b>U.S. Vessel</b>	<p>A vessel that:</p> <ul style="list-style-type: none"> <li>• Is documented under 46 USC 12101-12124 (Certificate of Documentation).</li> <li>• Is numbered as provided by 46 USC 12301-12309 (Certificate of Number).</li> <li>• Is owned in whole or part by a U.S. citizen or national and not registered in another country.</li> <li>• Was once documented under U.S. law and, without approval of the U.S. Maritime Administration, had either been sold to a non-U.S. citizen or placed under foreign registry or flag.</li> </ul>
<b>Use of Force Continuum</b>	A model for determining when and what types of force should be used in individual self-defense and law enforcement situations, except those involving action to compel a vessel to stop
<b>Vessel</b>	Every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water.
<b>Vessel Interdiction</b>	Detect, identify, evaluate and intercept TOIs; Implement End Game (e.g. stop, direct, board, search, seize/detain, arrest, neutralize/ destroy).
<b>Vessel without Nationality</b>	<p>Also referred to as a “stateless vessel”, a vessel that is not registered in one single nation. They are not entitled to fly the flag of any nation and, because they are not entitled to the protection of any nation, are subject to the jurisdiction of all nations. Nationality is evidenced by the following, all of which are considered affirmative claims under international law:</p> <ul style="list-style-type: none"> <li>• Oral claim of nationality by the master or other person in charge of the vessel</li> <li>• Vessel documents issued by the flag State</li> <li>• National flag or ensign flown</li> </ul>
<b>VOI</b>	Vessel of Interest: A vessel identified by the National Maritime Intelligence Center (NMIC), Area Maritime Intelligence Fusion Centers, District Intel. Office or other agency at the regional/port level as posing a potential security or criminal threat.
<b>VSO</b>	Vessel Security Officer: The person onboard the vessel, accountable to the Master, designated by the Company as responsible for security of the vessel, including implementation and maintenance of the Vessel Security Plan, and for liaison with the Facility Security Officer and the vessel’s Company Security Officer.
<b>VTS</b>	Vessel Traffic System: VTS is active in four major U. S. ports: New York, Puget Sound (Seattle), San Francisco, and Houston/Galveston. The system compresses radar, VHF-FM voice and video for transmission over commercial leased landlines or microwave and sends the information to the Vessel Traffic Center (VTC). The vessel data is processed and displayed in a graphical interface, a chart-based format that lends itself to early recognition of potentially dangerous situations. A minimum of 12 months of vessel transit data is stored in an Oracle database for later reconstructing collisions, spills or other incidences as well as data mining potentially used for studies like traffic density studies and port tonnage studies and fulfilling Freedom of

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-27
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

Information Act (FOIA) request.

**Vulnerability**

Measures the conditional probability of success given that a threat scenario occurs. It evaluates the adequacy and effectiveness of safeguards (both existing and proposed).

**Warning Shot**

A signal to a vessel to stop by firing ordnance; not a use of force.

**Waterfront Facilities**

Piers, wharves, docks, or similar structures to which vessels may be secured and naval yards, stations, and installations, including ranges; areas of land, water, or land and water under and in immediate proximity to them; buildings on them or contiguous to them and equipment and materials on or in them.

**Waterways Layer**

Waters within the U.S. Baseline, including navigable rivers and canals and any specified or designated internal waters.

**White Shipping**

Commercial, merchant, and fishing vessel shipping activity deemed to be neutral. That is, White Shipping is neither “BLUE”, which refers to a Friendly Force such as a Coast Guard asset, nor is it “RED,” which refers to a Hostile vessel.

**WMD**

Weapon of Mass Destruction: Any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; a disease organism; or radiation or radioactivity. (Source: COMDT Message Terms of Reference for Maritime Homeland Security [Draft V8], 18 USC § 2332a) Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. (Source: DOD Joint Pub 1-02)

VERSION DATE	V_1.1 26 MAY 2004	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9800-28
-----------------	-------------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

## Appendix 9920

This appendix outlines the purpose, agencies involved, and the scope of the Maritime Joint Task Force Memorandum of Understanding for voluntary cooperation and assistance on law enforcement in the Southeast Georgia and Northeast Florida Region.

### MARITIME JOINT TASK FORCE

#### MEMORANDUM OF UNDERSTANDING FOR VOLUNTARY COOPERATION AND ASSISTANCE ON LAW ENFORCEMENT

**A. PURPOSE.** The purpose of this Memorandum of Understanding (MOU) is to establish a systematic joint mission planning, leveraging, and de-conflicting process, ensuring the security of the southeast Georgia and northeast Florida region through enhanced coordination and cooperation among the signatory agencies. The systematic process outlined in this memorandum is intended to assure all agencies listed below: (1) jointly plan and conduct overlapping operations; (2) fully leverage each other's independent operations for mutual benefit; and (3) avoid unintentionally infringing upon each other's operations or unintentionally imposing redundant burdens on our customers.

Bureau of Customs and Border Protection  
Bureau of Immigration and Customs  
Enforcement  
Coast Guard Investigation Service  
Clay County Sheriff's Office  
Commander Carrier Group 6 (CARGRU 6)  
Commander Naval Region South East  
Commander Naval Surface Group 2  
Federal Bureau of Investigations  
Florida Department of Law Enforcement  
Florida State Health Department  
Florida Wildlife Conservation Committee  
Jacksonville Fire and Rescue

Jacksonville Sheriff's Office  
Nassau County Sheriff's Office  
Naval Air Station Jacksonville  
Naval Criminal Investigative Service  
Naval Station Mayport  
Putnam County Sheriff's Office  
Saint Augustine Police Department  
St. Johns County Sheriff's Office  
United States Coast Guard Group Mayport  
United States Coast Guard Marine Safety Office  
Jacksonville  
United States Marine Corps Blount Island  
Command

**B. SCOPE.** This MOU is to create an agreement for all signatory agencies to direct their staffs and subordinate commanders to consult with each other through the MJTF to conduct joint mission planning, leveraging, and de-conflicting processes in all cases for the operations listed in this section.

1. Homeland Security
2. Homeland Security Boarding Operations
3. Homeland Security Escort Operations
4. Homeland Security Zone Enforcement Operations
5. Multi-mission Afloat Patrol Operations

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9920-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

6. Marine Event Operations (including all permits, waterway closures, dredge permits, and safety zones)
7. Superbowl and Navy Sea and Sky Spectacular Operations
8. Heavy Weather Evacuation and Port Safety Planning, Exercises, and Operations
9. Military Outload Operations
10. Command Intelligence Liaison Activities
11. Military Security Liaison Activities
12. Security Resource Requests
13. Interagency Security Resource Coordination

The signatory agencies agree to alter their standard operation practices and issue such orders and directives as necessary to assure that all personnel responsible for designing and executing operations are aware the above missions must be conceived, designed, and executed through the joint mission planning and leverage all signatory agencies where practicable. As well, all signatory agencies agree to alter standard operating practices and issue such orders and directives as necessary to de-conflict operations. As such agencies will brief the MJTF on all operations that may possibly conflict with any agency's jurisdiction. Any agency that sees a possible conflict must contact the originating agency to explore de-conflicting processes.

The contents of this document augment and do not supercede existing law, regulations, and agency directives. Nothing in this agreement affects the statutorily prescribed duties and obligations under all applicable laws and regulations or the status of other active agreements between the Coast Guard and the State's law enforcement agencies.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	9920-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

# 10000 APPENDIX DANGEROUS CARGOES FOR SECURITY PLANNING

## 10010 Introduction

Federal law authorizes the Coast Guard to regulate the handling of dangerous cargo at waterfront facilities, the use of dangerous cargos on inspected vessels, and the carriage of certain specified liquid bulk cargoes by vessels. The Secretary of Treasury, at the request of the Secretary of Transportation, may refuse or revoke the clearance to enter a port of the United States when he believes a vessel carrying liquid bulk dangerous cargo or other hazardous materials has violated U.S. law. Vessels carrying dangerous cargoes are built and inspected to Coast Guard standards. Coast Guard marine inspectors conduct annual inspections to ensure these vessels meet and maintain these standards and make unannounced boardings to monitor transfers of dangerous cargos.

## 10011 Implications of Dangerous Cargoes in Security Planning

Planners must be proactive in designing security measures for vessels that carry dangerous cargoes and facilities that service those vessels. Both prevention and response must be taken into account when developing security plans. Using risk-based methodology, security measures should focus on those sectors of the maritime transportation system that have a higher risk of involvement in a Transportation Security Incident (TSI), including various tank vessels, barges, large passenger vessels, cargo vessels, towing vessels, offshore oil and gas platforms, and port facilities that handle certain kinds of dangerous cargoes or service such vessels.

## 10012 Scenario Based Planning

This section offers general security measure design guidance for planners to consider when developing facility or vessel security plans. Security planners should develop security measures, to mitigate the unique hazards associated with dangerous cargoes, for inclusion in security plans, on a scenario-specific basis. The following scenarios (at a minimum) are to be considered. This list is not intended to be all inclusive.

- Vessel carrying dangerous cargo underway in pilot waters
- Vessel handling dangerous cargo at a facility
- Facility/Pipeline vulnerabilities
- Over-ground Transportation, Truck/Train vulnerabilities

### 10012.1 Hazard Analysis and Inventory

Hazard analysis is a necessary component of comprehensive security planning. It is a three-step decision-making process comprised of hazard identification, vulnerability analysis, and risk analysis. This section focuses primarily on hazard identification. Hazard analysis is usually the task of an agency (e.g., the fire department, the Area Committee, or the LEPC) to review the hazard analysis information

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	10000-1
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

for their area.

The first task in conducting such an analysis is to complete an inventory of the dangerous cargoes the vessel or facility carries or handles to determine the nature of the hazard. This is a key step because it permits security planners to describe and evaluate risks, and to allocate resources accordingly. This information should be available to the security planner by examining the various inspection certificates/permits the facility or vessel holds. These materials include fuels and chemicals, such as chlorine, ammonia, and hydrochloric and sulfuric acids. Such materials should be given special attention (vulnerability analysis) in the planning process.

In this context, a hazard is any situation that is capable of causing injury or impairing an individual(s) health. During the process of identifying hazards, facilities or transportation routes will be pinpointed that contain materials that are potentially dangerous to humans. The identification of hazards also should provide information on:

- The types, quantities, and location(s) of hazardous materials at the facility, or transported through the facility; and
- The nature of the hazard that would accompany incidents, regardless of cause, such as explosions, spills, fires, and venting to the atmosphere.

Major transportation routes and transfer points at the facility, vessels in port, railroad yards, and trucking terminals, should also be included in the overall hazards identification plan. Risk analysis includes the probable damage that may occur if an incident involving dangerous cargoes occurs. Information that is necessary for risk analysis includes:

- The type of risk to humans, such as an acute, chronic, or delayed reaction.
- The groups that are most at risk.
- The type of risk to the environment, such as permanent damage or a recoverable condition.

## 10020 Database of Dangerous Cargoes

Detailed information on specific dangerous cargoes must be available to security planners when designing security measures. Input from responders to such incidents must be solicited as well, for inclusion into any plans developed to such end. [The Chemical Data Guide for Bulk Shipment by Water](#) contains important information on dangerous cargoes for use by the security planner. Information found within this link may be used for effective planning of prevention of, and response to, security incidents involving dangerous cargoes.

VERSION DATE	V_1.1 26 MAY 04	CLASSIFICATION: UNCLAS	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	10000-2
-----------------	--------------------	---------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------